HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Frau
Meike Dettmar

Konfiguration IT-forensischer Untersuchungspläne mittels wiederverwendbarer Methodenbausteine

2017

Fakultät Angewandte Computer- und
Biowissenschaften

BACHELORARBEIT

Konfiguration IT-forensischer Untersuchungspläne mittels wiederverwendbarer Methodenbausteine

Autor:
Frau Meike Dettmar

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
Fo14-w2-B

Erstprüfer:
Prof. Dr. rer. nat. Christian Hummert

Zweitprüfer:
Alexander Sigel, M. A.

Einreichung:
Mittweida, 27.11.2017

Faculty of Applied Computer and Biological Sciences

BACHELOR THESIS

Configuration of IT-forensic investigation plans using reusable method building blocks

author:
Ms. Meike Dettmar

course of studies:
General and Digital Forensics

seminar group:
Fo14 w2-B

first examiner:
Prof. Dr. rer. nat. Christian Hummert

second examiner:
Alexander Sigel, M. A.

submission:
Mittweida, 27.11.2017

Bibliografische Angaben:

Nachname, Vorname: Dettmar, Meike

Konfiguration IT-forensischer Untersuchungspläne mittels wiederverwendbarer Methodenbausteine

Configuration of IT-forensic investigation plans using reusable method building blocks

2017 - 69 Seiten

Mittweida, Hochschule Mittweida (FH), University of Applied Sciences,

Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2017

Abstract

Das Ziel der vorliegenden Bachelorarbeit war es, die in meinem hochschulinternen Praxisprojekt, eingereicht am 12.05.2017, generierten Bausteine zur automatischen Erstellung von IT-forensischen Untersuchungsplänen zu verbessern und weiterzuentwickeln, um so eine höhere Abdeckung von Fällen zu erreichen. Dazu wurde Literatur gesichtet und ein Interview mit Herrn Alexander Sigel, DigiTrace GmbH Köln, geführt. Das Praxisprojekt wurde ebenfalls von Herrn Sigel betreut.

In dieser Arbeit konnten erfolgreich neue Bausteine konfiguriert und bereits vorhandene Attribute von bestehenden Bausteinen sinnvoll erweitert werden. Die automatisch generierten Untersuchungspläne, ausgehend von diesen Bausteinen, können als Gedankenstütze oder Checkliste dienen und Fehler während der Untersuchung oder während der Erstellung des Untersuchungsplans minimieren. Durch die zielgerichtete Abfrage nach bestimmen Untersuchungszielen auf bestimmten zu untersuchenden IT-forensischen Geräten, Objekten, auf denen ein bestimmtes Betriebssystem installiert ist, können die ausgegebenen Untersuchungsschritte gezielt an den Untersuchungsauftrag angepasst werden.

Die Bachelorarbeit ist sowohl für Studierende als auch für selbstständige oder angestellte IT-Forensiker interessant, die im Zuge ihrer Arbeit Untersuchungspläne erstellen, um die Untersuchung systematisch zu gestalten.

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Diese Arbeit befasst sich mit der Konfiguration IT-forensischer Untersuchungspläne mittels wiederverwendbarer Methodenbausteine. Hierfür soll insbesondere die bereits vorhandene Bausteinliste, im Folgenden auch Bausteintabelle genannt, aus dem Praxisprojekt verbessert werden, sodass genauere Vorschläge für Untersuchungspläne entstehen. Gute Untersuchungspläne sorgen für ein strukturiertes Vorgehen und sind deshalb wichtig für gute Untersuchungen.

1.1 Problemstellung und Motivation zur Erstellung von Bausteinen für Untersuchungspläne

IT-forensische Untersuchungspläne bestehen aus geordneten Listen über auszuführende IT-forensische Teiltätigkeiten, Bausteinen. In der Praxis bei DigiTrace werden häufig Untersuchungspläne aufgestellt und im Projektverlauf aktualisiert. Das Auseinanderhalten und erneute Ordnen von bestehenden Untersuchungsschritten kann und soll hierbei sowohl für Geld- und Zeitersparnisse sorgen als auch die Wissensweitergabe an IT-Forensiker mit geringerer Berufserfahrung erleichtern.

Obwohl bei den in der Praxis meist manuell im Rahmen von Angeboten oder der Projektplanung erstellten Untersuchungsplänen verschiedene, auf der Textoberfläche unterschiedliche Ausprägungen vorkommen, können doch Bausteine abgegrenzt beschrieben und kategorisiert werden, was sie – wie Legobausteine – grundsätzlich wiederverwendbar und für neue Untersuchungspläne konfigurierbar macht. Dies wurde bereits im Praxisprojekt gezeigt. Diese Bausteine weisen zudem Beziehungen untereinander (beispielsweise Teiltätigkeit, verwandte Tätigkeit, Vorgänger, Nachfolger) auf, sowie zu weiteren Elementen, insbesondere zu den Untersuchungszielen, beziehungsweise Beweisfragen und zu IT-forensischen Methoden und Werkzeugen. Beispielsweise kann eine Relation einem Problem (zu untersuchenden Phänomen) eine oder mehrere geeignete Lösungen (Untersuchungsmethoden) zuordnen.

Im Unternehmen DigiTrace GmbH, Köln, besteht das Problem, dass das Wissen zu IT-forensischen Untersuchungen personengebunden ist. Mit der Erstellung von Baustei-

nen soll eine Wissensweitergabe, beziehungsweise Wissenswiederverwendung gewährleistet werden.

Zur Zeit ist es noch so, dass für jeden neuen Fall ein neuer Untersuchungsplan geschrieben wird, weshalb eine Art Serienfertigung angestrebt wird, die mittels einzelner Bausteine erreicht werden soll. Zusätzlich sollen Vorschläge für einzelne Schritte zu Untersuchungsfragen generiert werden, um das Wissen anderen, weniger berufserfahrenen Mitarbeitern einfacher zur Verfügung stellen zu können. [1]

1.2 Erster Bezug zum Praxisprojekt

Im Hochschulpraxisprojekt [2] vom 12.05.2017 wurden bereits geeignete Vorarbeiten zu wiederverwendbaren Methodenbausteinen zur Konfiguration IT-forensischer Untersuchungspläne geleistet, insbesondere in erster Näherung Inhalte geeigneter Methodenbausteine recherchiert und initial beschrieben, grob kategorisiert und in einem ersten einfachen Prototypen für die Erstellung und Wartung von Untersuchungsplänen erstmals verfügbar gemacht. Naturgemäß sind im damaligen Rahmen, der eher handlungspraktischer war und den Charakter einer Machbarkeitsstudie für die Umsetzung dieser Idee hatte, etliche Punkte nur angedacht worden und es blieben viele Fragen und Konkretisierungen offen. Daher wurde entschieden, dieses Thema im Rahmen dieser Bachelorarbeit in mehreren Aspekten systematischer und tiefgreifender zu bearbeiten. [1]

1.3 Aufgabenstellung und Ansatz

Ziel dieser Arbeit ist es Erfahrungswissen aus der Praxis und Literatur über IT-forensische Untersuchungspläne (einschließlich Incident Response) Methoden zu analysieren, Bausteine zu IT-forensischen Teiltätigkeiten geeigneter Granularität zu beschreiben und zu kategorisieren, geeignete Beziehungen der Bausteine untereinander und zu weiteren Elementen zu identifizieren und zu modellieren, insbesondere um durch deren Nutzung für IT-forensische Fragestellungen zu geeigneteren Untersuchungsplänen zu gelangen.

Zusätzlich soll ein Werkzeug, beispielsweise eine datenbankgestützte Anwendung, gefunden, entwickelt oder konfiguriert werden, die das gedankliche Gerüst aufnimmt und für Nutzung und Pflege praktisch verfügbar macht. Insbesondere soll diese für die Su-

che, Auswahl und Änderung von vernetzten Methodenbausteinen und deren Konfiguration, also den interaktiven Zusammenbau passender Teiltätigkeiten zu einem Gesamtplan, geeignet sein. Entwicklung eigener Software ist nicht Gegenstand dieser Arbeit.

Für den Anwendungsfall der Erstellung und Wartung solcher Untersuchungspläne soll argumentativ und mittels Walkthrough mit IT-Forensikern gezeigt werden, inwiefern das entwickelte gedankliche Gerüst wiederverwendbarer Bausteine einen IT-Forensiker in die Lage versetzt für verschiedene praxisrelevante Untersuchungsszenarien und damit einhergehenden Untersuchungszielen und Beweisfragen zu geeigneten Untersuchungsplänen zu kommen.

Weiterhin soll aufgezeigt werden welche Vorteile gegenüber manuell erstellten Plänen (beispielsweise durch Konsistenz, Standardisierung, Fehlervermeidung, systematische Gedankenstützen, Nutzung geeigneter Methoden) entstehen.

Gegenüber dem Praxisprojekt soll die Arbeit das Thema insbesondere hinsichtlich der Literaturrecherche und -auswertung, gegebenenfalls auch in verwandten Gebieten, aus denen sich Ideen auf Untersuchungspläne und Bausteine beziehen oder anwenden lassen, vertieft werden. Weiterhin sollen weitere Fallbeispiele und reale Untersuchungspläne, gegebenenfalls auch durch Befragung von IT-Forensikern bei DigiTrace, dafür sorgen, eine größere Anzahl von Bausteinen erstellen zu können, um eine höhere Abdeckung von Fällen zu erreichen und eine genauere, möglichst technikneutrale und zeitlich wenig veränderliche Beschreibung und Kategorisierung der Bausteine mit typisierten Beziehungen (Relationen) untereinander und zu anderen Bausteinen zu schaffen.

Insbesondere soll Erfahrungswissen darüber erhoben und modelliert werden, welche Bausteine sich für welche zu untersuchenden Sachverhalte besonders gut eignen. Ebenso sollen einfache Regeln formuliert werden (Bedingungen, Plausibilitätschecks, Erfahrungswissen), welche hinterlegt werden können, um auf der Basis vorheriger interaktiver Auswahlentscheidungen die Anwendbarkeit von Bausteinen zu steuern, beziehungsweise einzuschränken oder gar Hinweise für geeignete Bausteine zu geben. Ideen sollen fortentwickelt und Anforderungen aufgestellt werden. Die Mitwirkung an der Umsetzung eines bedienerfreundlicheren Konfigurationswerkzeugs soll stattfinden. Abschließend wird eine systematische Beschreibung der so erzielbaren und erzielten Vorteile entstehen. [1]

1.4 Fragestellungen und Hypothesen

1. "Wie gut ist die Abdeckung der relevanten Fälle und wie lässt sich diese mit Hilfe von Literaturdurchsicht verbessern?"

   Diese Frage zielt darauf ab herauszufinden, welche Bausteine bei der Praxisprojekt-Arbeit außer Acht gelassen oder übersehen wurden. Die Liste soll vollständiger und genauer werden, damit mehr Fälle abgedeckt werden können. Hierzu zählen auch Bausteine die bisher schon behandelt wurden, aber noch nicht alle für den Walkthrough verwendeten Szenarien abdeckten.

   H1: Die Abdeckung durch die Bausteine wird durch die Auswertung relevanter Literatur, durch Vergleiche mit vorhandenen Untersuchungsplänen und durch das Führen von Interviews erreicht.

2. "Welche Untersuchungsziele- und Fragen gibt es und welche davon sind wichtig für die Praxis bei DigiTrace?"

   Die Beantwortung dieser Frage dient dazu herauszufinden, für welche Untersuchungsziele es überhaupt Vorschläge zu erstellen gilt.

   H2: Eine bestimmte Menge von Untersuchungszielen kann ebenfalls durch vertiefte Recherche von Literatur und Untersuchungsberichten herausgefiltert und bei der Bausteinliste ergänzt werden.

3. "Wie kann man die Bausteine mit bestimmten Untersuchungsfragen in Zusammenhang bringen?"

   Diese Frage ist wichtig, da man nur mit der Korrelation aus Bausteinen und Untersuchungszielen dafür sorgen kann, dass ein wiederverwendbarer Untersuchungsplan entsteht.

   H3: In der Literatur und in den Berichten können Zusammenhänge von Untersuchungsmethoden- und Vorgängen, wie Untersuchungsfragen herausgefiltert werden, was es ermöglicht spezielle Bausteine bestimmten Untersuchungsfragen zuzuordnen und somit eine größere Anzahl solcher Korrelationen zu erreichen, was zu einer größeren Abdeckung von Untersuchungsfragen führt.

4. "Wie lassen sich, auf Basis der mit einem Werkzeug verwalteten Bausteine, für die Praxis geeignetere Vorschläge für Untersuchungspläne erstellen?"

Die Beantwortung dieser Frage dient dazu die Genauigkeit der durch die Datenbankabfragen ausgegebenen Untersuchungsvorschläge zu erhöhen.

H4: Wenn die Bausteinlisten bezüglich des Detailgrads ihrer Modellierung und ihrer Beschreibung angepasst wurden, können die Abfragen in beispielsweise einer datenbankgestützten Anwendung, auch ohne die Verwendung einer spezifischen GUI, verbessert werden. Eine bessere Modellierung der Bausteine und ihrer Beziehungen zueinander, auch unter Berücksichtigung von einfachen Regeln und Mustern, ermöglicht eine verbesserte Implementierung, was die Genauigkeit und Verwendbarkeit der vorgeschlagenen Untersuchungspläne erhöht und die Wissensweitergabe an weniger berufserfahrene IT-Forensiker erleichtert.

1.5 Gewähltes Vorgehen und Aufbau der Arbeit

Zunächst wurde fachliche Literatur zum Thema „Untersuchungspläne in der IT-Forensik“ und entsprechend zugehörige Sekundärliteratur bearbeitet, um hier weitere Bausteine zu finden, die eine Erweiterung der Bausteinliste ermöglichen könnten.

Anschließend wurde der aktuelle Kenntnisstand ausgehend vom Praxisprojekt-Bericht [2] erhoben, also die Ausgangsbasis für die Erweiterung der Bausteinliste geschaffen. Aufgrund der bearbeiteten Literatur und dem dazu folgenden Interview mit Alexander Sigel, DigiTrace GmbH, wurden die Bausteinlisten und die Bausteineigenschaften erweitert und ergänzt, was zu einer neuen Bausteinliste führte, die unter 3.4 zur Veranschaulichung in diese Arbeit eingefügt wurde.

Im Anschluss an diese Ergänzungen wurden erneut Tests, mittels bereits vorhandener Untersuchungspläne, für die generierten Listen durchgeführt, um die Abdeckung der generierten Untersuchungspläne zu testen und beurteilen zu können.

Unter 4. werden alle gesammelten Erkenntnisse und Vorgehen zusammengefasst und kritisch beurteilt.

Dementsprechend ergibt sich folgender Aufbau der Arbeit: Auswertung und kritische Würdigung von Literatur zu IT-forensischen Untersuchungen, Vorgehensweisen in der Praxis, daraus resultierende Bausteinergänzungen und erneute Testphasen für die erweiterte Bausteinliste. Abschließend fand eine Beurteilung derselbigen statt, die Arbeit wurde zusammengefasst, diskutiert und weitere zukünftige Arbeiten wurden aufgezeigt.

2 Auswertung und kritische Würdigung von Literatur zu IT-forensischen Untersuchungen

Nachfolgend wurde Literatur gesucht und bezüglich der unter 1.4 gestellten Fragen kritisch gewürdigt und befragt. Ebenso wurde die Literatur benutzt und befragt, um die verschiedenen Spalten der Bausteintabelle ergänzend zu füllen. Es wurde insbesondere nach Literatur aus den Gebieten „Untersuchungspläne in der IT-Forensik“ und angrenzenden Gebieten, wie: „Vorgehensmodelle in der IT-Forensik“ und „Software-Werkzeuge zur Verwaltung von Untersuchungsplänen und Fällen, sowie zur Verwaltung und interaktiven Nutzung von konfigurierbaren Plänen“ gesucht. Um an das Praxisprojekt anzuknüpfen werden zunächst typische, in der Literatur dargestellte, Anwendungsfälle und Vorgehensmodelle, sowie das daraus erstellte eigene Vorgehensmodell vorgestellt. Im Anschluss daran werden typische, in der Literatur dargestellte, Anwendungsfälle vorgestellt, die unter 3.3 mit den üblicherweise bei DigiTrace untersuchten Fällen abgeglichen werden, um die Spalte „Untersuchungsziel“ der Bausteine sinnvoll erweitern zu können. Sowohl die verwendete, als auch die nicht zitierte, aber für Zukunftsprojekte möglicherweise dennoch nützliche Literatur wird unter 2.3 kritisch gewürdigt. Zusätzlich wurde die nützliche Verwendung von Case-Management-Software, zusätzlich zur bereits bestehenden Datenbankanwendung, in Betracht gezogen und analysiert.

2.1 Vorstellung der in der Literatur dargestellten Vorgehensmodelle IT-forensischer Untersuchungen

Es gibt verschiedene Vorgehensmodelle, einige davon wurden bereits in der Praxisarbeit vorgestellt und behandelt, wie beispielsweise das Vorgehensmodell des Bundesamts für Sicherheit in der Informationstechnik (Bundesamt für die Sicherheit in der Informationstechnik [3], S. 62) und das Modell von Deloitte [4], ab S. 9.

Aus den verschiedenen Vorgehensmodellen wurde im Zuge des Praxisprojekt-Berichts ein eigenes Vorgehensmodell entwickelt:

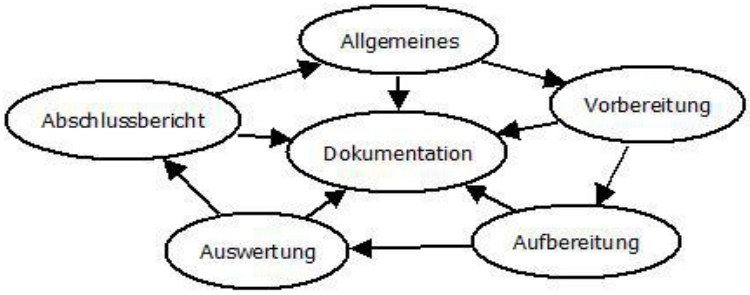

Abbildung 1: Eigenes erstelltes Vorgehensmodell

Weitere Literatur in der ähnliche Vorgehensweisen vorgestellt werden: „What Is Computer Forensics? [5], „Cyber Forensic Investigation Plan“ [6], S.1 f., „Taxonomy Of Computer Forensics Methodologies And Procedures for Digital Evidence Seizure“ [7], S. 3, „Examining The Data“ [8], S. 1-4 und „Mapping Process of Digital Forensic Investigation Framework“ [9], S. 4.

Allgemeine Vorgehensmodelle für explizite Fälle von „Incident Response“ lassen sich in „Computer Security Incident Handling Guide“ [10], S. 27, „Developing a Response Plan for Computer Forensics“ [11], S. 1 und „Digital Forensics Investigation Plan“ [12] ,S. 4 finden.

2.2 Aufzeigen typischer Anwendungsfälle für die Erweiterung der Bausteineigenschaften

In dem Buch „Computer Forensics Evidence Collection & Preservation“ von Course Technology [13] werden insbesondere folgende Untersuchungsziele aufgeführt und erläutert:

- Kindesmissbrauch, Kinderpornographie
- Hacking
- Systempenetrationen
- Passwort-Trafficking
- Fälschungen

- Diebstahl von Logos und Firmendarstellungen
- Häusliche Gewalt/Drohungen, Erpressung, Interneterpressung
- (Cyber-)Stalking
- Cyber-Mobbing
- Cyber-Verleumdung
- Glücksspiel
- Identitätsdiebstahl
- Diebstahl geistigen Eigentums
- Betäubungsmittelmissbrauch, Drogenhandel
- Betrug:
  - Manipulationsbetrug bei Software
  - Kreditkartenbetrug
  - Finanzbetrug
  - Falsche Kassenchecks
  - Online-Auktionsbetrug
  - Investitionsbetrug
  - Treuhandbetrug
  - Telekommunikationsbetrug
- Prostitution
- Softwarepiraterie
- Urheberpiraterie.
- Terrorismus
- Viren und Würmer
- Schäden an Netzwerken

- Unterschlagung
- Schuldenbeseitigung

Diese werden mit Hilfe eines Interviews unter 3.3 mit denen von DigiTrace abgeglichen und in den Bausteineigenschaften entsprechend sinnvoll ergänzt.

2.3 Kritische Würdigung zitierter Literatur und nicht zitierter Literatur

Bearbeitet wurde die oben genannte Literatur, die in ihren Teilaspekten zitiert wurde. Neben den oben genannten Punkten behandelte beispielsweise die wissenschaftliche Publikation „Digital Forensics Investigation Plan“ [12] folgende Themen: „Need for Digital Forensic Investigation“, dieser in dem Paper aufgeführte Punkt beinhaltet die Frage, warum IT-Forensik benötigt wird und wird in dieser Arbeit aufgrund des beschränkten Bearbeitungsrahmens nicht behandelt. Der Punkt „Digital Forensics Investigation Preparation Plan“ beinhaltet in diesem Paper allgemeine Punkte zum Umgang mit elektronischen Daten und IT-forensischen Fällen. Der letzte genannte Punkt „Data Evidence Identification Procedures“ beschäftigt sich mit den allgemeinen Anforderungen an einen IT-Forensiker und mit den Kompetenzen, die der Untersuchende haben sollte. Aus den genannten Gründen wurden diese Punkte insgesamt als „zu allgemein“ für diese Arbeit eingestuft. Ähnlich verhält es sich mit der Arbeit „Mapping Process of Digital Forensic Investigation Framework“ [9], die vor allem verschiedene andere Quellen im Bereich „Vorgehensweisen“ vergleicht, ähnlich wie es in dieser Arbeit unter 2.1 gemacht wurde. Dieser Punkt war im Praxisprojekt bereits abgeschlossen und fand deshalb nicht erneut Platz.

„Examining the Data“ [8] ist ebenfalls sehr allgemein gehalten. Dieser Bericht umfasst zwar einige forensische Vorgehensweisen, wie zum Beispiel „Stichwörter“, „Dateikopien und zuletzt geöffnete Dokumente“ oder „Zeitstempelanalyse“, allerdings enthielt das Paper keine Vorgänge die neue Erkenntnisse erbracht oder zu neuen Bausteinen geführt hätten.

Die Vortragsfolien über „Forensische Nutzung von IT und Daten“ von Deloitte Forensic [4] befasst sich neben dem oben vorgestellten Vorgehensmodell unter Anderem mit (Datenschutz)rechtlichen Gründen für IT-forensische Untersuchungen und ihren Rahmen. Der Punkt „Recht“ wurde aus Platzgründen aus der Arbeit ausgeklammert.

Ebenfalls in diesen Folien finden sich weiterhin allgemeine Ausführungen zu den einzelnen, bereits kurz ausgeführten Vorgehensschritten, aber auch hieraus ließen sich keine neuen Erkenntnisse gewinnen. Die Vortragsfolien mit dem Titel „Digital Evidence Collection Training for Law Enforcement“ [14] wurden aufgrund ihres großen Praxisbezugs unter 3.2 bearbeitet und die für die Bausteine wichtigen Punkte „Erweiterung der Bautseineigenschaften um den Aspekt „Lokalisation potentieller Beweismittel“ wurden hier behandelt. Weiterhin wird in den Vortragsfolien der allgemeine Umgang mit elektronischen Beweismitteln beschrieben und wo sich diese, beziehungsweise die dazugehörigen Geräte, befinden könnten. Das Buch „Computer Forensics – Evidence Collection & Preservation“ [13] beschreibt neben dem oben genannten „Vorgehensmodell“, wie sich Computerforensik in die heutige Zeit einfügt, wie ein computerforensisches Labor aussehen sollte und welches Equipment man für forensische Untersuchungen benötigt. Diese Informationen wurden ebenfalls ausgeklammert, da sie für diese Arbeit zu allgemein sind.

Im Bericht „FORZA: Digital Forensics Investigation Framework That Incorporate Legal Issues“ [15] werden insbesondere die einzelnen „w-Fragen“ aufgeschlüsselt und es werden mehr als die oben genannten „w-Fragen“ erzeugt, allerdings führt diese Aufschlüsselung von „w-Fragen“ für diese Arbeit zunächst zu weit.

„Developing a Response Plan for Computer Forensics“ [11] listet die einzelnen Untersuchungsschritte auf, wie bereits oben erwähnt und beschreibt diese kurz. Hier verhält es sich ähnlich wie bei „Mapping Process of Digital Forensic Investigation Framework“, die Erstellung eines eigenen Vorgehensmodells wurde bereis im Praxisprojekt abgeschlossen. Gleiches gilt für „What Is Computer Forensics?“ [5] und „Cyber Forensic Investigation Plan“ [6]. In letzterer wissenschaftlicher Publikation wird zusätzlich noch der „FTK-Imager“ als Auswertungswerkzeug für IT-forensische Untersuchungen vorgestellt.

Folgend wird bearbeitete Literatur, die fortführend aus bestimmten Gründen nicht zitiert und weiter verwendet wird, kritisch gewürdigt.

Literatur, die sich vorwiegend mit den Grundlagen allgemeiner oder digitaler Forensik und der Beweismittelerhebung befasst, siehe „Crime Scene Investigation“ [16] und „Applying Traditional Forensic Taxonomy To Digital Forensics“ [17], wurde aus der Arbeit ausgeklammert. „Taxonomy of computer forensics methodologies and procedures for digital evidence seizure“ [7] beschreibt neben den allgemeinen Phasen des IT-forensischen Vorgehens spezielle Methoden und deren Vor- und Nachteile, allerdings konnten aus dieser Literatur keine neuen Informationen für die Ergänzung der Bausteinliste

gezogen werden. Genauso verhält es sich mit „Computer Security Incident Handling Guide“ [10].

Das Dokument „Australian Forensic Computing“ [18] behandelt statistische Auswertungen darüber, welche Kompetenzen für IT-forensische Analysten wichtig sind. Auch dieser Themenbereich liegt aus Gründen des Bearbeitungsrahmens für diese Arbeit außerhalb der in der Arbeit behandelten Themen. In dem Forschungsbericht „Zielgerichtete Produktentwicklung durch modulare Prozessstrukturen und situationsgerechte Methodenauswahl“ [19] geht es weniger um IT-forensische Vorgänge als um die allgemeine Vorstellung von Prozess- und Phasenmodellen, um Problemlösungsstrategien zu verbessern. Insbesondere gibt es hier ein Modell das Eingangsartefakte, Tätigkeiten und Ausgangsartefakte beinhaltet. Da das bisherige Bausteinkonzept bereits auf einem ähnlichen Modell beruht (Artefakt und Methode als eigene Spalte innerhalb der Liste), wurde das Konzept ebenfalls nicht vertiefend verfolgt.

Aus dem Arbeitspapier „Support For Computer Forensics Examination Planning With Domain Modeling“ [20] geht kein besonderer Vorteil für eine mittels Domain Modeling organisierte Untersuchung hervor, allerdings wird „Case Domain Modeling“ an sich an dem Punkt der endgültigen Implementierung der Datenbank wieder wichtig, deshalb an dieser Stelle ebenfalls vorläufig ausgeklammert. Siehe auch 4.4 „Vorschläge für weiterführende Arbeiten“.

Die beiden wissenschaftlichen Paper „Attack Trees“ [21] und „How To Reuse Knowledge About Forensic Investigations“ [22] zielen darauf ab, Hypothesen zu erstellen, anhand derer man seinen Untersuchungsvorgang anpassen kann. In „Attack Trees“ geht es darum, einen Ausgangspunkt, zum Beispiel „Safe geknackt“ an die Spitze eines „Angriffsbaums“ zu setzen, dessen Blätter dann mit den verschiedenen Möglichkeiten einen Safe zu knacken befüllt werden. Dieses Vorgehen hätte man auf die digitale Forensik übertragen können, allerdings wurde das Überprüfen der Bausteinvorschläge mittels Praxistests als sinnvoller empfunden. In „How To Reuse Knowledge about Forensic Investigations“ geht es um die schriftliche Formulierung von Hypothesen, also werden hier im Prinzip die Möglichkeiten aus den „Blättern“ ausformuliert. Das Vorgehen ähnelt dem vorherigen.

Schließlich wurden alternative Implementierungsmöglichkeiten zusätzlich zur Datenbank gesucht. Vorschläge zu Case-Management-Software wurden der Homepage „Whodunnit“ [23] entnommen, allerdings waren die meisten der hier vorgeschlagenen Werkzeuge für den Gebrauch vor Ort (Digital Notepads, Case Notes) gedacht und sind für diese Arbeit deshalb nicht unmittelbar verwendbar. Das Aufstellen von Untersu-

chungsplänen und auch deren nachgelagerte Wartung kann aber auch Bestandteil von anderen Case-Management-Systemen, wie zum Beispiel „Foreman“ (https://www.theforeman.org/, zuletzt abgerufen am 24.11.2017) oder „SirenTec“ (http://sirentec.com/, zuletzt abgerufen am 24.11.2017), sein. Diese Tools arbeiten häufig mit zeitlichen Rahmen, weshalb sie für die Untersuchung an sich gut geeignet sein können. Für die allgemeine Bestimmung von Untersuchungsabläufen, wie in dieser Arbeit vorgestellt, sind sie daher weniger gut geeignet.

Die Literatur, die für die Weiterentwicklung der Bausteine verwendet werden konnte, wurde bereits unter den Punkten 2.1 und 2.2 zitiert. Nachfolgend findet sich für die Bausteinerweiterung genutzte Literatur, zusammen mit den Resultaten, unter den Punkten 3.2 und 3.3.

3 Vorgehensweisen in der Praxis

Zunächst wird unter 3.1 klargestellt auf welchem Kenntnisstand, ausgehend vom Stand des Praxisprojekts (12.05.2017) [2], diese Arbeit aufbaut. Dann werden Punkte aus der Literatur ausgewertet, die für die Anpassung der Bausteine verwendet werden konnten. Die aus der Literatur entnommenen Untersuchungsziele, aufgeführt unter 2.2, werden unter 3.2 mit Hilfe eines Interviews mit dem erfahrenen IT-Forensiker Alexander Sigel, DigiTrace GmbH, Köln, abgeglichen. Nachfolgend werden die gänzlich neu generierten Bausteine vorgestellt und vorab verschiedenen Anwendungsfällen zugeordnet. Anschließend durchläuft die neu generierte Bausteinliste erneut Tests bezüglich ihrer Verwendbarkeit auf bereits vorhandene Untersuchungspläne.

Die Ausgabe der Untersuchungspläne wurde weiterhin mit „MySQL“ durchgeführt.

3.1 Bisherige Erkenntnisse basierend auf der Praxisarbeit

Bisher konnten die Bausteine in verschiedene Kategorien: "Allgemeines", "Vorbereitung", "Aufbereitung" und "Auswertung" eingeteilt werden. Ergänzend könnte man "Abschlussbericht" und "Dokumentation" einfügen.

„Vorbereitung“ beinhaltet bis jetzt die Bausteine „Datenquellen“, „Datensicherung“, „Erstaufnahme“, „Hardwarekomponenten“, „IT-Infrastruktur“, „Logserver“, „Nämlichkeit“, „Personennetzwerk“ und „Projektskizze“.

„Aufbereitung“ beinhaltet bis jetzt die Bausteine „Backups“, „Betriebssystem“, „Carving“, „Dateisystem“, „Entschlüsselung“, „Filterung“, „Formatkonvertierung“, „Partitionierung“ und „Schattenkopien“.

Die Kategorie „Auswertung“ beinhaltet aktuell die Bausteine „Erweiterte Attribute“, „Anrufprotokolle“, „Arbeitsspeicher“, „Bewegungsprofil“, „Bewertung“, „E-Mails“, „Erstsichtung“, „Eventlogs“, „externe Geräte“, „Fileslack-Analyse“, „Internetaktivität“, „Kommunikationsprotokolle“, „Konfigurationsdateien“, „laufende Prozesse“, „Live-Forensik“, „Malwareprüfung“, „Metadaten“, „Post-mortem-Analyse“, „Registry“, „Signaturprüfung“, „Sitzungsdaten“, „SMS/MMS“, „Software“, „Stichwortsuche“, „Suchindex“, „Systemzeit“, „Userdaten“ und „Zeitstempelanalyse“. Diese Bausteine sind alle Teil von IT-forensischen Untersuchungen.

Details zu den Bausteininhalten können dem Praxisprojekt-Bericht entnommen werden.

Der Aufbau der bisherigen Datenbankabfragen sieht bisher wie folgt aus:

1. Abfrage für Betriebssysteme die sich auf einem Client befinden können:

```
use methodenbausteine;

select objekte.ObjName, group_concat(betriebssysteme.BSName separator'/') as Objekte from objekte, betriebssysteme, bs_obj
  where objekte.ObjIndex = bs_obj.ObjIndex
  AND
        betriebssysteme.BSIndex = bs_obj.BSIndex AND
        objekte.ObjName = "Client";
```

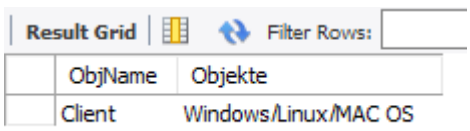

Abbildung 2: Bisherige Betriebssysteme die auf einem Client laufen können

3. Abfrage für Objekte die Windows als Betriebssystem nutzen:

```
use methodenbausteine;

select betriebssysteme.BSName, group_concat(objekte.ObjName separator'/') as Objekte from betriebssysteme, objekte, bs_obj

  where objekte.ObjIndex = bs_obj.ObjIndex

  AND

        betriebssysteme.BSIndex = bs_obj.BSIndex AND

        betriebssysteme.BSName = "Windows";
```

	BSName	Objekte
	Windows	Client/Tablet/Server/externe Festplatte

Abbildung 3: Bisherige Objekte die Windows als Betriebssystem nutzen

4. Abfrage für bestimmtes Untersuchungsziel

```
use methodenbausteine;

select BauName, Bname, ZielName from bausteine, bau_ziel, untersuchungsziel

 where

bau_ziel.ZielIndex = untersuchungsziel.ZielIndex

And

bausteine.BauIndex = bau_ziel.BauIndex

aND

untersuchungsziel.ZielName = "Datenabfluss";
```

BauName	Bname	ZielName
Erstaufnahme	Vorbereitung	Datenabfluss
Projektskizze	Vorbereitung	Datenabfluss
IT-Infrastruktur	Vorbereitung	Datenabfluss
zentraler Logserver	Vorbereitung	Datenabfluss
Personennetzwerk	Vorbereitung	Datenabfluss
Identifikation von Datenquellen	Vorbereitung	Datenabfluss
Sicherung	Vorbereitung	Datenabfluss
Nämlichkeit	Vorbereitung	Datenabfluss
Hardwarekomponenten	Vorbereitung	Datenabfluss
Hashwertvergleich	Allgemeines	Datenabfluss
Hintergrundrecherchen	Allgemeines	Datenabfluss
Dateisystem	Aufbereitung	Datenabfluss
Partitionierung	Aufbereitung	Datenabfluss
Betriebssystem	Aufbereitung	Datenabfluss
Carving	Aufbereitung	Datenabfluss
Schattenkopien	Aufbereitung	Datenabfluss
Wiederherstellung aus Backups	Aufbereitung	Datenabfluss
Entschlüsselung	Aufbereitung	Datenabfluss
Filterung	Aufbereitung	Datenabfluss
Formatkonvertierung	Aufbereitung	Datenabfluss
Suchindex	Auswertung	Datenabfluss
Live-Forensik	Auswertung	Datenabfluss
laufende Prozesse	Auswertung	Datenabfluss
Arbeitsspeicher	Auswertung	Datenabfluss
Post-mortem-Analyse	Auswertung	Datenabfluss
Malwareprüfung	Auswertung	Datenabfluss
User	Auswertung	Datenabfluss
Software	Auswertung	Datenabfluss

Abbildung 4: Bisherige Untersuchungsschritt-Ausgabe für ein bestimmtes Problem, hier: Datenabfluss Teil 1

externe Geräte	Auswertung	Datenabfluss
Sitzungsdaten	Auswertung	Datenabfluss
Kommunikationsprotokolldaten	Auswertung	Datenabfluss
Systemzeit	Auswertung	Datenabfluss
Eventlogs	Auswertung	Datenabfluss
Registry	Auswertung	Datenabfluss
Konfigurationsdateien	Auswertung	Datenabfluss
Stichwortsuche	Auswertung	Datenabfluss
Dateisignaturprüfung	Auswertung	Datenabfluss
Metadaten	Auswertung	Datenabfluss
Alternate Data Streams	Auswertung	Datenabfluss
E-Mail-Client	Auswertung	Datenabfluss
Zeitstempelanalyse	Auswertung	Datenabfluss
Anrufprotokolle	Auswertung	Datenabfluss
SMS/MMS	Auswertung	Datenabfluss
Erstsichtung	Auswertung	Datenabfluss

Abbildung 5: Bisherige Untersuchungsschritt-Ausgabe für ein bestimmtes Problem, hier: Datenabfluss Teil 2

5. Client, Linux, Datenabfluss:

```
use methodenbausteine;


select bausteine.BauName, bausteine.Bname, objekte.ObjName, be-
triebssysteme.BSName, untersuchungsziel.ZielName

from bausteine, objekte, betriebssysteme, untersuchungsziel,
bau_obj, bau_bs, bau_ziel, obj_bs

 where     bausteine.BauIndex = bau_obj.BauIndex
 And  bausteine.BauIndex = bau_bs.BauIndex
 And  bausteine.BauIndex = bau_ziel.BauIndex
 And  bau_obj.BauIndex = bau_bs.BauIndex
 And  bau_obj.BauIndex = bau_ziel.BauIndex
 And  bau_bs.BauIndex = bau_ziel.BauIndex
 And  objekte.ObjIndex = obj_bs.ObjIndex
 And  objekte.ObjIndex = bau_obj.ObjIndex
 And  obj_bs.ObjIndex = bau_obj.ObjIndex
 And  betriebssysteme.BSIndex = bau_bs.BSIndex
 And  betriebssysteme.BSIndex = obj_bs.BSIndex
 And  bau_bs.BSIndex = obj_bs.BSIndex
 And  untersuchungsziel.ZielIndex = bau_ziel.ZielIndex
 And
        objekte.ObjName = "Client"
        And
        betriebssysteme.BSName = "Linux"
        And
        untersuchungsziel.ZielName = "Datenabfluss";
```

BauName	Bname	ObjName	BSName	ZielName
Hashwertvergleich	Allgemeines	Client	Linux	Datenabfluss
Hintergrundrecherchen	Allgemeines	Client	Linux	Datenabfluss
Dateisystem	Aufbereitung	Client	Linux	Datenabfluss
Partitionierung	Aufbereitung	Client	Linux	Datenabfluss
Carving	Aufbereitung	Client	Linux	Datenabfluss
Schattenkopien	Aufbereitung	Client	Linux	Datenabfluss
Wiederherstellung aus Backups	Aufbereitung	Client	Linux	Datenabfluss
Entschlüsselung	Aufbereitung	Client	Linux	Datenabfluss
Filterung	Aufbereitung	Client	Linux	Datenabfluss
Formatkonvertierung	Aufbereitung	Client	Linux	Datenabfluss
Arbeitsspeicher	Auswertung	Client	Linux	Datenabfluss
Post-mortem-Analyse	Auswertung	Client	Linux	Datenabfluss
Malwareprüfung	Auswertung	Client	Linux	Datenabfluss
User	Auswertung	Client	Linux	Datenabfluss
Software	Auswertung	Client	Linux	Datenabfluss
externe Geräte	Auswertung	Client	Linux	Datenabfluss
Sitzungsdaten	Auswertung	Client	Linux	Datenabfluss
Kommunikationsprotokolldaten	Auswertung	Client	Linux	Datenabfluss
Systemzeit	Auswertung	Client	Linux	Datenabfluss
Eventlogs	Auswertung	Client	Linux	Datenabfluss
Registry	Auswertung	Client	Linux	Datenabfluss
Konfigurationsdateien	Auswertung	Client	Linux	Datenabfluss
Dateisignaturprüfung	Auswertung	Client	Linux	Datenabfluss
Metadaten	Auswertung	Client	Linux	Datenabfluss
Alternate Data Streams	Auswertung	Client	Linux	Datenabfluss
Zeitstempelanalyse	Auswertung	Client	Linux	Datenabfluss
Anrufprotokolle	Auswertung	Client	Linux	Datenabfluss
Suchindex	Auswertung	Client	Linux	Datenabfluss
Live-Forensik	Auswertung	Client	Linux	Datenabfluss
laufende Prozesse	Auswertung	Client	Linux	Datenabfluss
Erstaufnahme	Vorbereitung	Client	Linux	Datenabfluss
Projektskizze	Vorbereitung	Client	Linux	Datenabfluss
IT-Infrastruktur	Vorbereitung	Client	Linux	Datenabfluss
zentraler Logserver	Vorbereitung	Client	Linux	Datenabfluss
Personennetzwerk	Vorbereitung	Client	Linux	Datenabfluss
Identifikation von Datenquellen	Vorbereitung	Client	Linux	Datenabfluss
Sicherung	Vorbereitung	Client	Linux	Datenabfluss
Nämlichkeit	Vorbereitung	Client	Linux	Datenabfluss
Hardwarekomponenten	Vorbereitung	Client	Linux	Datenabfluss

Abbildung 6: Bisherige Ausgabe der Datenbankabfrage für ein spezifisches Problem auf einem bestimmten Gerät mit einem bestimmten Betriebssystem

3.2 Erweiterung der Bausteineigenschaften um den Aspekt “Lokalisation potentieller Beweismittel”

Interessant ist die Frage der Lokalisation potentieller Beweismittel vor allem, da angestrebt wird die Untersuchungsfragen auf zu untersuchende Objekte zu beziehen und diese noch genauer zu gestalten.

Generell sind Beweismittel auf elektronischen Geräten zu finden und jede auf ihnen gespeicherte Information ist ein potentielles Beweismittel. Einige Geräte erfordern möglicherweise interne oder externe Netzteile, damit man die gespeicherten Informationen erhalten kann [14].

Für erste Tests bereits vorhandene zu Untersuchende Geräte waren: „Client“, „Handy“, „Tablet“, „Server“ und „externe Festplatte“.

Da "Client" der Oberbegriff für Laptops, PCs, MACs, Desktop PCs, MAC Minis, Imacs etc. ist, wurde die Entscheidung getroffen diesen Punkt nicht im einzelnen zu unterteilen.

Aus Gründen der IT-Sicherheitsaspekte "Spiegelung des Netzwerkverkehrs" und "Sicherheitslücken, Fernzugriffsmöglichkeiten", wurde das Objekt "Netzwerk" als solches ergänzt.

Zu ergänzende Objekte bei "externen Festplatten" wären externe Geräte im Allgemeinen, also USB-Sticks, Speicherkarten und andere Wechselmedien. Speicherkarten können in vielen Geräten enthalten sein und deshalb übergreifend auf Kamera-, Computer-, Handy-, Audiowiedergabegerät-, PDA-, Videospielkonsolen- und Handhelduntersuchungen sinnvoll sein.

Die Objekte "USB-Stick" und "Speicherkarte" wurden ergänzt.

Im Allgemeinen können alle möglichen anschließbaren Peripheriegeräte, wie Grafikkarten, Netzwerkkarten, Mäuse, Tastaturen, Soundkarten, Festplatten, RAID-Controller, CD-ROM-, DVD-, oder BD-ROM-Laufwerke/Brenner, Diskettenlaufwerke, TV-Karten, Monitore, Bluetooth oder Infrarotschnittstellen (USB), Lautsprecher und Mikrofone (auf mobilen Geräten meist intern verbaut), Speicherkartenlesegeräte, Webcams, Touchpads, Trackballs, Drucker, Faxgeräte, Kopierer, Gamepads, Gamecontroller, Grafiktabletts, Headsets, Joysticks, Lenkräder, NAS-Speicher, Plotter, Scanner, Sensor, USB-

Hubs, USB-Sticks, Videoprojektoren, CNC-Maschinen, KVM-Switches, Telefone, Kartenlese-Adapter, Kreditkartenleser, Modems, Wireless Network Access Points, Directional Antennas, ZIP-drive-Lesegeräte, Handheld Scanner, biometrische Lesegeräte, USB-Stick-Kopierer und GPS-Empfänger Spuren hinterlassen.

Die Metadaten für alle Peripheriegeräte erhält man für gewöhnlich aber durch Untersuchung entsprechender Dateien auf dem Gerät an dem sie angeschlossen waren. Trotzdem wurden aus dieser Liste aller Peripheriegeräte die Geräte extrahiert, die potentiell eigene "Objekte" darstellen können, da sie selbst über potentiell zu untersuchende Daten verfügen: "interne Festplatte", als Abgrenzung zu "externe Festplatte", "Interne Festplatten" können auch im "Client" angeschlossene Festplatten sein, möglicherweise sind diese jedoch nicht direkt auf den ersten Blick erkennbar. "Drucker", "Kopiergerät", "Scanner", "CNC-Maschine", "Telefon" und "GPS-Empfänger" wurden aus dieser Liste ebenfalls extrahiert und ergänzt, da sie durchaus als eigene Daten- und Informationsträger fungieren können.

"NAS-Speicher" wurden als Unterpunkt von "Server" nicht explizit aufgelistet.

Andere Quellen für digitale Beweise können weiterhin sein: Videokameras, Digitalkameras, Audiorekorder und Anrufbeantworter, Videorekorder, Receiver und Zugangskarten, Überwachungskameras, Spielekonsolen, Videospiele, SIM-Kartenleser, MP3- und Audiospieler, Chat-Devices, Telefonsysteme, Haushaltsgeräte, Kraftfahrzeugelektronik, Wasserfahrzeugelektronik, GPS, Computerchips, Pager, Scanner, Fax-Maschinen, Festplattenkopiergeräte und Router. [14]

Aus dieser Liste wurden die Objekte "Kamera", "Rekorder", "Receiver", "Konsole", "Wiedergabegerät", "Haushaltsgerät" und "Fahrzeugelektronik" extrahiert.

Die vollständige Liste von zu untersuchenden Objekten lautet also wie folgt: "Client", "Handy", "Tablet", "Server", "externe Festplatte", "interne Festplatte", "Netzwerk", "USB-Stick", "Speicherkarte", "Drucker", "Kopiergerät", "Scanner", "CNC-Maschine", "Telefon", "Kamera", "Rekorder", "Receiver", "Konsole", "Wiedergabegerät", "Haushaltsgerät", "Fahrzeugelektronik".

3.3 Erweiterung der Bausteine auf der Basis typischer Anwendungsfälle bei DigiTrace

Im Bezug auf die unter 2.2 aufgeführten Untersuchungsziele, führte ich ein Interview mit Herrn Alexander Sigel, in welchem ich ihn zu den explizit in der Literatur aufgeführten Fällen befragte und inwiefern diese eine Rolle im DigiTrace-Alltag spielen. Behandelte Fälle seien zum Beispiel kinderpornografische Inhalte, vor allem im Zusammenhang mit deren Verbreitung und Besitz.

Die Analyse solcher Fälle erfordere insbesondere zusätzliche Hashwertvergleiche oder spezifische Softwareentwicklung (siehe auch Abschnitt 3.5). Auch würden nicht-richtlinienkonformer Gebrauch von IT-Geräten und Software, Systemsabotage, vor allem im Rahmen von Zerstörung (physische Gewalteinwirkung, Löschungen, Verschlüsselungen), Untersuchung von Fälschungen, Untersuchung von Buchhaltungs- und Rechnungssystemen, Abrechnungsbetrug, physische Androhung von Gewalt und Erpressung (Lösegeldforderungen, Cybermobbing und -stalking), welche spezielle Methoden erfordern können (Erstellung von Honeypots, nachladbaren Pixeln zur Identifikation der Quell-IP-Adresse, siehe auch Abschnitt 3.5) untersucht. Im Bezug auf Erpressungsfälle gehe es vor allem um Erpressungs- also Verschlüsselungstrojaner, beispielsweise „(Non-)Petya“ und „Wannacry“. Hier müsse geklärt werden, wie das System infiziert wurde, von wo der Angriff kam und ob er gerichtet oder ungerichtet stattfand. Auch müsse das Schadensausmaß geklärt werden (siehe Abschnitt 3.5) Im Anschluss an solche Angriffe sei es wichtig, die verloren gegangenen Daten soweit wie möglich wiederherzustellen, um den Schaden so gut es geht zu begrenzen. Im Anschluss daran solle eine Richtlinienerstellung oder Richtlinienverbesserung stattfinden. Der Punkt „Richtlinienerstellung“ wurde allerdings nicht als neuer Baustein erstellt, da er zu sehr im Bereich der IT-Sicherheit liegt.

Häufig im Unternehmen behandelte Fälle seien Fälle von Daten-Diebstahl (Exfiltration). Hier gelte es, potentielle Verbindungen zu Dritten zu klären und zu untersuchen, ob Daten kopiert und/oder gesendet wurden. Mutmaßliche vertrauliche Informationen werden hierbei mittels Stichwortsuchen gefiltert. Ebenfalls festgestellt werden sollte, ob auf bestimmte Dateien unberechtigter Zugriff erfolgte, beispielsweise werde dies durch Registryanalysen, LNK-Dateianalysen und Durchsicht von Jumplists, sowie der Indexierung der Windows.edb durchgeführt. Auch kämen Fälle von Identitätsdiebstahl (Impersonifikation) vor, bei der sich eine Person als eine andere ausgebe, zum Beispiel durch

Nutzung dessen Mail- oder Chatkonten, sowie durch Social Engineering. Auch durch Diebstahl betroffen sei geistiges Eigentum im Bereich Software, was Software- und Codevergleiche (siehe auch Abschnitt 3.5) nach sich ziehe.

Ebenfalls ginge es um IT-Sabotage im Allgemeinen, also beispielsweise unerlaubte Webinterface-Zugriffe und die generelle Frage nach der Sicherung der IT-Systeme.

Herr Sigel ist langjähriger Spezialist in der Aufklärung von Wirtschaftskriminalität. Hierzu zählen beispielsweise Bilanzmanipulation, Rechnungsfälschung, Unterschlagung, Insolvenzverschleppung über strafbare Handlungen zum Nachteil von Unternehmen bis hin zu Korruption, also Non-Compilance. Untersuchungen hierzu benötigen Fragebögen, Datenbankrecherchen und Hintergrundrecherchen zu Personen und Unternehmen (Corporate Intelligence). Auch gilt es, Informationen aus öffentlich verfügbaren Datenquellen in Bezug zu Informationen aus forensischen und IT-forensischen Fällen zu setzen und insbesondere auffällige Beziehungen und Verflechtungen zwischen Personen und Unternehmen zu visualisieren.

Im Bereich Untersuchung von Urheberrechtsverletzungen gehe es um Feststellungen zu Art und Umfang potentiell urheberrechtlich geschützten Materials, um Software-Plagiate, aber auch um die Beurteilung, ob ein zur Feststellung etwaiger Urheberrechtsverletzungen verwendetes automatisiertes IT-System korrekt arbeitet.

Bei Untersuchungen zum Thema mutwillige Schädigung eines Unternehmens geht es um Manipulation von Telefonanlagen, also Missbrauch zur Leistungserschleichung und zur Verschleierung des wahren Täters. Des Weiteren können hier Untersuchungen zur Ausspähung oder zum unberechtigten Mithören von Gesprächen stattfinden. Hier ist vor allem die Frage zu klären, wie jemand in das System eindringen konnte (Sicherheitslücken, Fernzugriffsmöglichkeiten).

Der letzte aus der Literatur zitierte Untersuchungsgrund ist der der Schuldenbeseitigung. Im Grunde genommen werden hier wieder Straftaten verübt, die zum finanziellen Vorteil desjenigen stattfinden, wie Unterschlagung oder Dokumentenfälschung. Hier sollte geprüft werden, ob ein Geldproblem vorliegt (Finanzdaten).

Weitere unternehmenswichtige Untersuchungen sind beispielsweise das Beurteilen anderer forensischer Gutachten, das Prüfen, ob eine vollständige Datenlöschung stattgefunden hat, falls sie angefordert wurde. Klärung der diesbezüglichen Fragen: War es möglich die Daten zu löschen und wenn nicht, warum nicht? Und wenn doch, wie? Bei Kontaktverboten kann geprüft werden, ob Kontakt bestand, obwohl er nicht hätte be-

stehen sollen. Es wird generell geprüft, ob gerichtliche Anordnungen eingehalten wurden oder nicht. Auch Untersuchungen von Fahrzeugelektronik gäbe es, beispielsweise von Bordcomputern oder Dashcams bei Unfällen, auch wenn solche Fälle bislang bei DigiTrace noch nicht bearbeitet wurden. Des Weiteren kann hier der Fehlerspeicher ausgelesen werden. Das Fahrzeug kann auf Tachomanipulation und Versicherungsbetrug hin untersucht werden. Wurden die Fahrtenbücher gewissenhaft geführt? Weitere Tätigkeiten sind im Allgemeinen: Eingangskontrolle, Plausibilisierung (Plausibilisierung, Zeitstempelanalyse), Datenrettung logischer und physischer Beschädigungen (Rekonstruktion, Carving), inhaltliche Sichtung und Bewertung großer Mengen von Dokumenten und E-Mails (Review im Rahmen von eDiscovery, auf erster und zweiter Review-Stufe, Indexierung, inhaltlicher review (e-Discovery) (intellektuelle Beurteilung; Methode), Triage (Identifikation von Datenquellen, Triage) als Ersteinschätzung der Relevanz von Datenquellen oder -bereichen noch während der Erstuntersuchung, Tests virtueller Umgebungen bezüglich hinterlassener Spuren (Experimente).

Welche Untersuchungsfälle wurden für die Bausteinliste aus der oben erstellten Aufzählung extrahiert?

"Untersuchungsziel" beinhaltet aktuell unter Anderem die Punkte "unzulässige Nutzung", "Datenabfluss", "Malware" und "Betrug". Dieser Punkt beinhaltet allerdings auch das oben aufgelistete "Hacking", weshalb dieser Punkt nicht explizit aufgeführt wird. Der Punkt "Betrug" beinhaltet alle oben aufgelisteten Formen des selbigen. "Besitz illegaler Daten" beinhaltet auch den Besitz von kinderpornographischen Inhalten oder urhebergeschützten Materialien. Zusätzlich ergänzt wurden "Erpressung", "Identitätsdiebstahl" und "Diebstahl geistigen Eigentums". Die Punkte "Stalking, Glücksspiel und Prostitution" wurden ausgeklammert, da sie in der DigiTrace-Praxis nicht häufig untersucht werden.

Die vollständige Liste der Rubrik "Untersuchungsziel" sieht wie folgt aus: "unzulässige Nutzung", "Datenabfluss", "Malware", "Betrug", "Besitz illegaler Dateien", "Erpressung", "Identitätsdiebstahl", "Diebstahl geistigen Eigentums" und „Belästigung“.

3.4 Vorstellung neu generierter Bausteine

Die bestehenden Bausteine wurden größtenteils so belassen, wie sie waren. Der bisherigen Bausteintabelle wurde eine Spalte "Voraussetzung" eingefügt, um festzuhalten, dass es für manche Untersuchungsschritte nötig ist, zuvor andere Schritte durchzuführen, wie beispielsweise eine Festplatte vor der Auswertung an sich zu entschlüsseln, also eine Art hierarchische Zuordnung neben der bereits vorhandenen Reihenfolge "Allgemeines, Vorbereitung, Aufbereitung, Auswertung". Entschlüsselung ist ein bereits existierender Baustein, zu dem es jetzt eine Referenz gibt.

Der Schritt "Schattenkopien" wurde in "Systemabbilder" umbenannt, um den Untersuchungsschritt allgemeiner zu gestalten und eine Betriebssystemunabhängigkeit zu schaffen.

Neu generierte oder erweiterte Bausteine sind:

- "Erstaufnahme, Beweisfrageformulierung"

"Beweisfrageformulierung" wurde dem Baustein "Erstaufnahme" ergänzt, da die Beweisfragen von Beginn an nicht immer klar vom Auftraggeber formuliert werden.

- "Identifikation von Datenquellen, Triage"

"Triage" wurde dem Baustein "Identifikation von Datenquellen" hinzugefügt, da es bei „Triage“ vornehmlich darum geht, relevante Datenquellen zu selektieren, das heißt die wichtig erscheinenden werden von den unwichtig erscheinenden bereits vor dem Stattfinden der eigentlichen Untersuchung getrennt.

- "Systemabbilder"

Der Baustein "Schattenkopien" wurde in "Systemabbilder" umbenannt, um ihn betriebssystemneutraler zu gestalten, auch wenn die meisten durchgeführten Untersuchungen Windows-spezifisch sind.

- "Rekonstruktion, Carving"

"Rekonstruktion" wurde dem Baustein "Carving" angefügt, da sich "Carving" spezifisch auf die Wiederherstellung von Dateien bezieht. Rekonstruktion im Allgemeinen ist

durchaus aber auch ein wichtiger Punkt, im Rahmen von beispielsweise virtuellen Maschinen oder RAIDs.

- „Schädlingsidentifikation“

„Schädlingsidentifikation“ zielt darauf ab, herauszufinden, welche Art von Malware das zu untersuchende System befallen hat, wenn es befallen wurde, um die Wahrscheinlichkeit auf eine Entschlüsselung zu erhöhen und das Problem definieren und beschreiben zu können.

- „Nachvollziehen des Verschlüsselungsablaufs“

Dieser Schritt ist notwendig, um potentielle Einfallstore genauer einzugrenzen und die Identifikation von Datenquellen genauer zu ermöglichen.

- "Cloudspeicher"

Dieser Untersuchungsschritt bezieht sich auf die Auswertung von in Clouds gespeicherten Daten oder Backups.

- „E-Mail-Client, Webmailer"

„Webmailer" könnte als Punkt zu "Internetaktivität" zählen, so wie "E-Mail" im Allgemeinen auch. Allerdings sind die Punkte "E-Mail" und "Internetaktivität" aufgrund von unterschiedlichen Untersuchungsmethoden und Datenmengen durchaus von einander zu trennen. Zur E-Mail-Auswertung zählen zudem nicht nur E-Mail-Software sondern eben auch "Webmailer", also Online-Webdienste.

- „Plausibilisierung, Zeitstempelanalyse"

Die „Zeitstempelanalyse“ war vorher ein alleinstehender Untersuchungsschritt, ist aber im Allgemeinen Teil der Plausibilisierung, weshalb sie dem neu generierten Schritt „Plausibilisierung“ nachgestellt wurde.

- „Audio-, Video- und Bilddateien“

„Audio-, Video- und Bilddateien" waren im Praxisprojekt zuerst als Einzelpunkt angedacht, wurden in der ersten Bausteinausführung allerdings wieder verworfen, da sich einige andere Untersuchungsschritte, beispielsweise „Hashwertvergleiche" auf diese Dateien als „Artefakte" beziehen. Dennoch kann es andere, untersuchungsrelevante Informationen hierzu geben. Damit diese nicht verloren oder untergehen, wurde der Punkt ergänzend hinzugefügt.

- „Passwortdateien“

Bei diesem Untersuchungsschritt geht es darum relevante Passwörter, in Dokumenten oder den ihnen zugehörigen Dateien, ausfindig und nutzbar zu machen.

- „Finanzdaten"

Dieser Schritt erfordert Einsicht in Finanzakten eines Verdächtigen oder Geschädigten, um beispielsweise Betrugs- und Erpressungsfälle im finanziellen Bereich nachvollziehen zu können.

- "Sicherheitslücken, Fernzugriffsmöglichkeiten"

Der Punkt "Sicherheitslücken, Fernzugriffsmöglichkeiten" wurde als komplett neuer Punkt der Untersuchungsbausteinliste hinzugefügt und war vorher nicht vorhanden, da er sich eher im Bereich "IT-Sicherheit" als im Bereich "forensische Auswertung" bewegt, allerdings ist der Punkt trotzdem Teil der täglichen Arbeit und hängt passiv mit IT-Sicherheitsvorfällen zusammen, die zu IT-forensischen Untersuchungen führen, weshalb er ergänzt wurde. Im Zusammenhang mit Untersuchungen, die Sicherheitsvorfälle betreffen, ist es wichtig herauszufinden, wie der Vorfall zu Stande kommen konnte.

- "Täterprofilanalyse"

Der Punkt "Täterprofilanalyse" wurde ebenfalls komplett neu erstellt und beinhaltet die Suche nach einem Täter auf der Basis von gefundenen Hinweisen und Fakten, zum Beispiel im Bezug auf Datenklau oder Erpressung. In solchen Fällen ist es wichtig zu evaluieren, welche Beweggründe und Motive der potentielle Täter hatte.

- "Experimente"

"Experimente" waren ebenfalls noch nicht in der Bausteinliste vorhanden und wurden ergänzt, da in einigen Fällen, zum Beispiel bei der Analyse von Malware oder Software, getestet wird wie diese Programme arbeiten und was für Spuren sie hinterlassen.

- „"Fallen" für Systemeindringlinge“

Bezieht sich zum Beispiel auf die Spiegelung des Netzwerkverkehrs, die Erstellung von Honeypots oder nachladbaren Pixeln. Dies ist genauso wie "Sicherheitslücken, Fernzugriffe" ein Untersuchungsschritt, der sich auf IT-Sicherheit bezieht, aber dennoch während einer IT-forensischen Untersuchung Anwendung finden kann. Den Netzwerkver-

kehr zu spiegeln, Honeypots zu erstellen oder nachladbare Pixel einzufügen kann dafür sorgen, einen Täter in eine Falle zu locken und dadurch zu stellen.

- "Softwareentwicklung"

"Softwareentwicklung" ist auch kein Punkt der IT-forensischen Auswertung an sich, ist aber dennoch ein Teil der IT-forensischen Untersuchung in ihrer Gesamtheit. So wurde in der Praxis beispielsweise Software entwickelt, um Standbilder aus Videos zu extrahieren. Dieser Untersuchungsschritt findet seinen Platz in der Kategorie „Allgemeines“.

- "Telefonanlagen"

Auch dieser Punkt wurde im Zuge dieser Arbeit ergänzt, obwohl er, so wie einige andere Listenpunkte auch, nicht direkt zur IT-forensischen Analyse zählt. Auch hier ist der Grund der Ergänzung, dass er durchaus ein Teil des Untersuchungsumfangs sein kann. Möglicherweise sind an Telefonanlagen Abhöreinrichtungen angebracht oder die Telefonanlagen sind spezifisch konfiguriert.

- "Bestimmung des Schadensausmaßes"

Die "Bestimmung des Schadensausmaßes" zählt zur IT-forensischen Analyse, vor allem im Bereich von Malware oder Datenabfluss und kann durchaus ein Teil des Untersuchungsauftrags an sich sein.

- "Software-/Codevergleich"

„Software-/Codevergleich“ zählt zum Bereich "Diebstahl geistigen Eigentums" und dient vor allem dazu herauszufinden, ob Code kopiert und somit gegen das Urheberrecht verstoßen wurde. Auch dieser Untersuchungsschritt hat mit der IT-forensischen Untersuchung im klassischen Sinne nichts zu tun und ist eher ein gesonderter Untersuchungsauftrag, wurde der Vollständigkeit halber aber dennoch ergänzt.

Trotzdem sind IT-forensische Untersuchungen denkbar, in denen Codevergleich, aber vor allem Softwarevergleich zum Tragen kommen.

- „Datenanforderung“

Dieser Punkt fällt ebenfalls unter die Kategorie „Allgemeines“ und soll den Fall abdecken, dass Daten von außerhalb angefordert werden müssen, um Daten und Ereignisse zu plausibilisieren und zu beurteilen, sowie vergleichen zu können.

Die neue Bausteinliste enthält jetzt insgesamt 61 Untersuchungsschritte, nach Beendigung des Praxisprojekts waren es 46. Die Abdeckung für Untersuchungspläne und

-vorschläge durch die Erstellung neuer Bausteine konnte also verbessert werden. Einige der Bausteine, zum Beispiel "Erstaufnahme, Beweisfrageformulierung", „Identifikation von Datenquellen, Triage“, oder "Rekonstruktion, Carving", bekamen durch die Ergänzung ihres Titels eine höhere Genauigkeit und einen größeren Umfang. Vor allem der Bereich „Malwareanalyse“ und somit auch Untesuchungen im Bereich „Incident Response“ lässt sich durch die Erstellung von Bausteinen, wie "Bestimmung des Schadensausmaßes", „Schädlingsidentifikation“, oder „Nachvollziehen des Verschlüsselungsablaufs“ in seinen einzelnen Untersuchungsschritten besser beschreiben und nachvollziehen. Ebenso wurde für diesen Fall das Vorhandensein eines Täters durch die Bausteine „Täterprofilanalyse“ und „“Fallen“ für Systemeindringlinge“ nicht ausgeschlossen. Für den Fall, dass sich dieser Umstand im Laufe einer Untersuchung ergeben sollte, stellen diese Bausteine weitere Optionen für sinnvolle Untersuchungen dar und bieten so ein Maß an Flexibilität.

3.5 Weitere Ergänzungen der Bausteinliste

Kurz- und Langbeschreibung wurden aus Übersichts- und Platzgründen zu einem einzelnen Feld "Beschreibung" zusammengefasst. Hierfür wurden die zusätzlichen Informationen aus der Spalte "lange Beschreibung" in das Feld "kurze Beschreibung" hinzugefügt. Im Anschluss daran wurde die Spalte "lange Beschreibung" gelöscht und die Spalte "kurze Beschreibung" in "Beschreibung" umbenannt, sodass es hier nicht zu Informationsverlust kommt.

Der Bereich "Allgemeines" bestand aus den Bausteinen "Hashwertvergleich" und "Hintergrundrecherchen". Ergänzt wurden hier die Bausteine "Experimente", "Softwareentwicklung" und "Datenanforderung".

"Passwortdateien" wurde sowohl dem Bereich "Allgemeines" als auch dem Bereich "Auswertung" zugeordnet, da Passwörter sowohl vor der Sicherung als auch während der Untersuchung an sich von Bedeutung sein können.

Der Bereich "Vorbereitung" besteht nach wie vor aus den Bausteinen "Erstaufnahme, Beweisfrageformulierung", "Projektskizze", "IT-Infrastruktur", "zentraler Logserver", "Personennetzwerk", "Identifikation von Datenquellen, Triage", "Sicherung, Imaging", "Nämlichkeit" und "Hardwarekomponenten". Außer zwei Namensänderungen gab es hier keine wesentlichen Veränderungen.

Im Bereich "Aufbereitung" haben sich die Bausteine "Dateisystem", "Partitionierung", "Wiederherstellung aus Backups", "Entschlüsselung", "Formatkonvertierung" und "Be-

triebssystem" befunden. Geändert wurden die Bausteine "Carving" zu "Rekonstruktion, Carving", "Schattenkopien" zu "Systemabbilder", um ihn betriebssystemneutraler zu halten und "Filterung" zu "Filterung und Datenreduktion", um andere Methoden zur Datenreduktion neben der Filterung nicht zu vergessen oder zu vernachlässigen.

Der Bereich Auswertung beinhaltete die Bausteine "Suchindex", "Erstsichtung", "Live-Forensik", "laufende Prozesse", "Arbeitsspeicher", "Post-mortem-Analyse", "Malwareprüfung", "User", "Software", "externe Geräte", "Sitzungsdaten", "Kommunikationsprotokolldaten", "Systemzeit", "Registry", "Konfigurationsdateien", "Stichwortsuche", "Dateisignaturprüfung", "Metadaten", "erweiterte Attribute", "Fileslack-Analyse", "Internetaktivität", "Anrufprotokolle" und "SMS/MMS". Geändert und ergänzt wurden folgende Bausteine: "Eventlogs" zu "Systemaktivitäten, Eventlogs", um genauso wie bei "Systemabbilder" eine Betriebssystemunabhängigkeit zu schaffen. "E-Mail-Client" zu "E-Mail-Client, Webmailer", um diese ergänzend explizit zu nennen. "Audio-, Video- und Bilddateien", "Täterprofilanalyse", "Telefonanlagen", "Schadensausmaß", "Software-/Codevergleich", "Schädlingsidentifikation", "Verschlüsselungsablauf", "Cloud-Speicher", "Finanzdaten" und "Lokalisation" wurden dem Bereich hinzugefügt.

Eine gänzlich neu erschaffene Kategorie ist die "IT-Sicherheit", da sie nicht zwingend Teil einer IT-forensischen Untersuchung sein muss, aber kann, weshalb hier zwei Bausteine grob ergänzt wurden: "Sicherheitslücken, Fernzugriffsmöglichkeiten", „"Fallen" für Systemeindringlinge".

Ebenfalls gänzlich neu hinzugefügt wurde die Spalte "Voraussetzung", um die Reihenfolge der Bausteine festlegen zu können und um zu zeigen, welche Voraussetzungen nötig sind, um diesen Schritt auszuführen.

So ist für den Baustein "Erstaufnahme, Beweisfragenformulierung" erst ein Auftrag nötig.

Eine "Projektskizze" muss nur angelegt werden, wenn das Projekt die nötige Größe hat, deshalb hat dieser Baustein die Voraussetzung "großes Projekt, e-Discovery-Fall, Incident Response Fall".

In alle unmittelbar auf die Erstaufnahme folgenden Bausteine wurde die Voraussetzung „Erstaufnahme“ eingefügt.

Diese ist ebenfalls für alle anderen Bausteine notwendig, allerdings ist die Untersuchung, wenn man sich an Bausteinen anderer Bereiche bedient, bereits soweit fortgeschritten, dass auf die fortwährende Wiederholung der „Erstaufnahme“ für diese Bausteine in der Spalte „Voraussetzung“ verzichtet wurde. Diese Wiederholung findet also

nur innerhalb eines Bausteinbereichs, in diesem Fall "Vorbereitung" statt, um den Bereichen in sich eine bestimmte Reihenfolge und somit eine bestimmte Hierarchie zuzuschreiben.

Als erster Baustein des Untersuchungsplans überhaupt hat "Erstaufnahme, Beweisfragenformulierung" nur den Auftrag als Voraussetzung, ohne Auftrag gäbe es keinen Untersuchungsplan. "Projektskizze" und "IT-Infrastruktur" haben jeweils die Voraussetzungen "großes Projekt", "e-Discovery-Fall", "Incident Response Fall", "Erstaufnahme". "Identifikation von Datenquellen, Triage" hat die Voraussetzungen "Erstaufnahme, Beweisfragenformulierung", "Projektskizze", "IT-Infrastruktur" und "Datenquellen sind nicht eindeutig", was wiederum ebenso auf "großes Projekt", "e-Discovery-Fall" und "Incident Response Fall" hindeuten kann, aber die Identifikation von Datenquellen kann schon bei einem kleineren Fall durchaus undurchsichtig sein, weshalb diese Punkte hier nicht explizit aufgelistet wurden. "Sicherung, Imaging" kann stattfinden nachdem die Datenquellen identifiziert sind, sofern nötige Soft- und Hardware für das zu untersuchende Objekt vorhanden sind und deren Nämlichkeit überprüft wurde. Die Nämlichkeit hat die Voraussetzungen "Erstaufnahme", "Beweisfragenformulierung" und "Identifikation von Datenquellen". "Hardwarekomponenten“ hat die Voraussetzungen "Identifikation von Datenquellen". In dem Bereich "Allgemeines" hat "Hashwertvergleich" die Voraussetzung "zu vergleichende Daten vorhanden" und bezieht sich damit auf alle anderen Bausteine, deren Untersuchungsergebnisse einen Hashwertvergleich ermöglichen. "Hintergrundrecherchen" hat die Voraussetzung "Mehr Wissen benötigt". "Experimente" hat die Voraussetzung "Notwendigkeit für das Verstehen von Abläufen". "Softwareentwicklung" hat die Voraussetzung "Keine bereits existierende Software für das Problem benutzbar". "Datenanforderung" hat die Voraussetzung "Andere Datenquellen als Untersuchungsergänzung benötigt". Im Bereich "Aufbereitung" haben die Bausteine "Dateisystem", "Partitionierung" und "Betriebssystem" die Voraussetzung "Sicherung". Der Baustein "Rekonstruktion, Carving" hat die Voraussetzung "gelöschte Dateien vermutlich vorhanden, ein Netzwerksystem muss rekonstruiert werden (RAID)". "Systemabbilder" und "Wiederherstellung aus Backups" haben die Voraussetzung "System muss oder soll, beispielsweise wegen Zerstörung, wiederhergestellt werden". "Entschlüsselung" hat die Voraussetzungen "Verschlüsselung vorhanden" und "Passwortdokumente". "Filterung, Datenreduktion" setzt voraus, dass die Untersuchungsfragen klar sind und somit auch das Untersuchungsziel. Damit man Verwendung für den Baustein "Formatkonvertierung“ hat, braucht man "Probleme bezüglich der Lesbarkeit von anderen Dateiformaten".

Der Baustein "Suchindex" aus dem Bereich "Auswertung" hat die Voraussetzungen "großer Fall", "e-Discovery-Fall", "Klarheit, wonach gesucht wird“. Die "Erstsichtung" hat die Voraussetzung "Entschlüsselung, falls verschlüsselt". Um "Live-Forensik" durchzuführen braucht man die "Notwendigkeit von Incident Response oder "erster Hilfe" vor Ort am eingeschalteten System".

Die beiden Bausteine "laufende Prozesse" und "Arbeitsspeicher" haben die Voraussetzung "Live-Forensik". Die "Post-mortem-Analyse" hat die Voraussetzung "Sicherung". Die Malwareprüfung hat die Voraussetzung "Malwarebefall vermutet".

Die Bausteine "User", "Software", "Sitzungsdaten", "Kommunikationsprotokolldaten", "Systemzeit", "Systemaktivitäten, Eventlogs", "Registry", "Konfigurationsdateien", "Internetaktivität" und "Plausibilisierung, Zeitstempelanalyse" haben allesamt die Voraussetzung "Ursachenforschung".

All diese Bausteine sind in fast jeder Untersuchung gegenwärtig und es gibt viele verschiedene Gründe sie zu nutzen, sodass eine unmittelbare "Voraussetzung" nicht notwendig ist. Die Verwendung liegt vielmehr in der fallspezifisch angepassten Selektion durch den Untersuchenden.

Der Untersuchungsschritt "externe Geräte" hat die Voraussetzung "Datentransfer vermutet". Die "Stichwortsuche" hat die Voraussetzung "Beweisfragen und Untersuchungsziele sind klar". Die "Dateisingnaturprüfung" setzt voraus, dass eine Dateimanipulation vermutet wird, die Verwendung des Bausteins "Metadaten" verlangt, dass interessante, prüfbare Dateien vorhanden sind.

"Erweiterte Attribute" werden zum Beispiel bei Verdacht auf versteckte Dateien auf dem Datenträger untersucht. Die "Fileslack-Analyse" kann durchgeführt werden, wenn die "Prüfung auf Restexistenz relevanter Daten notwendig" erscheint. Sowohl die "Anrufprotokolle" als auch die "SMS/MMS"-Untersuchungen sind dann von Belang, wenn ein "interessanter Kontakt zwischen zwei oder mehr Personen vermutet wird".

Bei der Analyse von "Audio-, Video- und Bilddateien" wird meist nach "bestimmten Dateien" gesucht. Die "Täterprofilanalyse" kommt selbstverständlich nur dann zum Einsatz, wenn es Hinweise und Spuren auf einen Täter gibt, anhand derer man ihn analysieren kann. Die "Telefonanlagen" werden dann untersucht, wenn eine "Vermutung auf Fehlkonfiguration oder Abhöreinrichtungen" vorhanden ist.

Die „Schätzung des Schadensausmaßes“ kommt immer dann zustande, wenn ein Datenverlust zu beklagen ist. Der "Software-/Codevergleich" kommt beispielsweise beim "Verdacht auf Diebstahl geistigen Eigentums" zum Einsatz.

Die Punkte "Schädlingsidentifikation" und "Verschlüsselungsablauf" finden dann Verwendung, wenn Malware oder sonstige Verschlüsselungssoftware auf dem Zielsystem vorhanden ist. Nach "Cloud-Speichern" wird geschaut, wenn man Anspruch auf lückenlose, vollständige Datenerhebung hat. Die "Finanzdaten" können dann ausgewertet werden, wenn man Zugriff auf diese erhält, also wenn die Situation die Überprüfung dieser Dateien zulässt. Die "Lokalisation" des Täters kann man durchführen, wenn man in der Lage war, die IP-Adresse oder die GPS-Koordinaten nach Deutschland zurückzuverfolgen.

Die beiden Bausteine "Sicherheitslücken, Fernzugriffsmöglichkeiten" und „"Fallen" für Systemeindringlinge" aus dem Bereich "IT-Sicherheit" haben die Voraussetzungen "Sicherheitsvorfall" und "merkwürdige Netzwerkaktivitäten, Vermutung auf Systemeindringling".

Die Ziele, Artefakte und Methoden der neu generierten Bausteine wurden ebenfalls in die Liste eingefügt.

Nachfolgend werden explizit die Bausteine genannt, bei denen unter "Objekt" nicht alle "Objekte“ aufgelistet sind:

- "IT-Infrastruktur": da diese nur in Netzwerken oder eventuell durch Kommunikationsprotokolldaten auf Clients, Servern oder Haushaltsgeräten ("Smart Home") erschlossen werden kann.
- "zentraler Logserver": auch dieser ist nur im Netzwerk notwendig, wenn Daten zentral gesammelt werden müssen.
- "Hashwertvergleich". da nicht auf allen neu hinzugefügten Objekten Dateien gefunden werden können, die für einen solchen sinnvoll oder hilfreich wären.
- "Dateisystem", "Partitionierung", "Betriebssystem". da auch hier nicht alle Objekte gut auswertbare Dateisysteme, Partitionierungen oder Betriebssysteme haben.
- "User", "Software", "externe Geräte", "Sitzungsdaten", "Kommunikationsprotokolldaten". da nicht alle der aufgelisteten Objekte über ein offenes Userinterface verfügen, welches einem das Anlegen von Nutzern oder Installieren eigener Software erlaubt. Somit muss man hier auch auf "Sitzungsdaten" verzichten. Des Weiteren sind manche der aufgelisteten Objekte bereits selbst "externe Geräte", an welche keine weiteren "externen Geräte" angeschlossen werden

können, somit muss man ebenso auf "Kommunikationsprotokolldaten" verzichten.

- "Registry". nicht alle aufgelisteten Objekte sind dafür gemacht unter einem Windows-Betriebssystem zu laufen.
- "E-Mail-Client, Webmailer", "Anrufprotokolle", "SMS/MMS": nicht alle aufgelisteten Objekte sind darauf ausgelegt, E-Mail-Verkehr, SMS/MMS oder Anrufe zu senden oder zu empfangen.
- „"Fallen" für Systemeindringlinge": bezieht sich ebenfalls auf eine Netzwerkumgebung.
- "Telefonanlagen": bezieht sich nur auf das Objekt "Telefon".
- "Schadensausmaß": bezieht sich auf Geräte, auf denen potentiell wichtige Informationen gespeichert sind, was nicht auf alle Objekte zutrifft.
- "Software-/Codevergleich": bezieht sich auf Geräte, auf denen potentiell Software und- oder Code gespeichert werden würde.
- "Verschlüsselungsablauf": bezieht sich auf Objekte, auf denen sich potentiell wichtige Daten befinden und die deshalb von einer Verschlüsselung betroffen wären.
- "Cloud-Speicher": hier sind nicht alle aufgelisteten Objekte darauf ausgelegt Verbindungen zu einem Cloud-Speicher aufzunehmen.
- "Passwortdateien": werden nicht auf jedem der aufgelisteten Objekte abgelegt.
- "Lokalisation": hierfür eignen sich ebenfalls nicht alle aufgeführten Objekte.

Natürlich ist es möglich jedes der aufgeführten Objekte zweckentfremdend zu manipulieren. In diesen Beispielen wurde von stereotypischen Verwendungen ausgegangen und solche "Sonderanfertigungen" wurden ausgeklammert.

Die Spalte "Betriebssystem" blieb unverändert.

Nachfolgend sind explizit alle Bausteine aufgelistet, die nicht alle Untersuchungsziele enthalten:

- "Schädlingsidentifikation": Anwendung nur bei Malware

- "Verschlüsselungsablauf": Anwendung nur bei Malware
- "Finanzdaten": Anwendung nur bei Betrug, Erpressung

Allen anderen Bausteinen konnte ein möglicher Wert für alle hinzugefügten Untersuchungsziele zugeteilt werden. Sollte man im Laufe der Testphasen feststellen, dass einige Bausteine für bestimmte Untersuchungen irrelevant sind, kann man das Untersuchungsziel im Nachhinein noch entfernen. Würde man die Untersuchungsziele bereits jetzt radikal beschneiden und nicht im vorgeschlagenen Untersuchungsplan manuell selektieren, dann bestünde die Gefahr, dass einige Bausteine für bestimmte Untersuchungsziele bereits vergessen würden, bevor sie überhaupt zu ihrem Einsatz fänden.

3.6 Präsentation der neuen Bausteinliste

Nummer	Name	Beschreibung	Bereich	Voraussetzung	Ziel	Artefakt	Methode	Objekt	Betriebssystem	Untersuchungsziel
10	Hashwertvergleich	Erstellung und Vergleich der Hashwerte (SHA, MD5) von Software oder Datenträgerkopien	Allgemeines	zu vergleichende Daten vorhanden	Eindeutige Übereinstimmungen von Software, Daten und Datenträgerkopien sicherstellen	Dateien auf zu untersuchenden Datenquellen, Imagekopie, Audio-, Video- und Bilddateien, Software	Prüfsummen generieren und abgleichen	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, CD/DVD, Kamera, Rekorder, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
11	Hintergrundrecherchen	Nachforschungen zu bestimmten, beispielsweise Softwarebasierten Inhalten, Viren oder Beweisfragen im Allgemeinen	Allgemeines	Mehr Wissen benötigt	Fallverständnis erweitern	fallbezogene Unklarheiten	Rücksprache mit Klient, Internetsuche, nachlesen	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
50	Experimente	Mit beispielsweise Software, Viren oder Würmern experimentieren	Allgemeines	Notwendigkeit für das Verstehen von Abläufen	Ablaufverständnis erweitern	Malware, Software, Decrypter	Nachstellung von Szenarien und intellektuelle Auswertung der daraus resultierenden Ergebnisse	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
52	Softwareentwicklung	Entwicklung von Software für gewisse forensische Notwendigkeiten, beispielsweise Extraktion von Standbildern aus Videos	Allgemeines	Keine bereits existierende Software für das Problem benutzbar	IT-forensische Auswertung und deren Ergebnisse optimieren		Softwareentwicklung	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
58	Datenanforderung	Anforderung von Daten, beispielsweise eines Providers, um sie mit den gefundenen Daten abgleichen zu können	Allgemeines	Andere Datenquellen als Untersuchungsergänzung	Daten anfordern, um sie mit gefundenen Daten abzugleichen	Kommunikationsprotokolle	Per E-Mail oder Telefon Möglichkeiten für Datenweitergabe erfragen	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung

Abbildung 7: Teil 1 der Bausteintabelle, Bereich: Allgemeines

Nummer	Name	Beschreibung	Bereich	Voraussetzung	Ziel	Artefakt	Methode	Objekt	Betriebssystem	Untersuchungsziel
60	Passwortdateien	Suche nach Passwortdateien oder Erfragen derselbigen zum einloggen in diversen Applikationen oder Diensten	Allgemeines, Auswertung	Entschlüsselung notwendig	Passwortdateien ausfindig machen, um eine Entschlüsselung zu ermöglichen	Dokumente, SAM, shadow, passwd	Suche nach Passwörtern in einschlägigen Betriebsdatenbanken oder Dokumenten, Erfragen von Passwörtern beim Kunden	Client, Handy, Tablet, Server, interne Festplatte, USB-Stick, Speicherkarte, Konsole, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung

Abbildung 8: Teil 2 der Bausteintabelle, Bereich: Allgemeines, Vorbereitung

Nummer	Name	Beschreibung	Bereich	Voraussetzung	Ziel	Artefakt	Methode	Objekt	Betriebssystem	Untersuchungsziel
1	Erstaufnahme, Beweisfragenformulierung	Klärung des Sachverhalts und des Untersuchungsgegenstands, welche Beweisfragen sollen bearbeitet werden?	Vorbereitung	Auftrag	Ausmachen, welche Artefakte und Objekte untersucht werden sollten und welche Sachverhalte geklärt werden sollen		Rücksprache mit Klient	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
2	Projektskizze	Übersicht über den Ablauf des Projekts erstellen	Vorbereitung	großes Projekt, e-Discovery-Fall, Incident Response Fall, Erstaufnahme	Strukturierung des Projektablaufs, Übersicht über Tätigkeiten gewinnen		intellektuelle Analyse	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
3	IT-Infrastruktur	Erheben und verstehen wesentlicher Informationen zur IT-Infrastruktur, um potentiell relevante Datenbestände zu identifizieren, zum Beispiel: Netzwerkplan, Clientlisten, Softwareausstattung,...	Vorbereitung	großes Projekt, e-Discovery-Fall, Incident Response Fall, Erstaufnahme	Zuordnung von Personen zu Clients, physische Standorte fallrelevanter Untersuchungsobjekte ausmachen, Zugriffsmöglichkeiten und Netzwerkzugänge auf und von Clients und Server von innen und außen evaluieren		Rücksprache mit Klient	Client, Netzwerk, Server, Haushaltsgerät	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
4	zentraler Logserver	Einrichtung eines zentralen Logservers	Vorbereitung	großes Projekt, e-Discovery-Fall, Incident Response Fall, zentrale Datensammlung nötig, IT-Infrastruktur	Sicherung von Logfiles zur sicheren Verwahrung während und nach einem Vorfall	Logfiles	Eigenen Server im Klienten-Netzwerk zwischenschalten, auf dem Logdateien abgelegt werden	Client, Netzwerk, Server	Windows, Linux, MAC OS	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
5	Personennetzwerk	Erstellung einer Übersicht über alle beteiligten Personen und deren Verbindung zueinander	Vorbereitung	großes Projekt, e-Discovery-Fall, Incident Response Fall, Erstaufnahme	Fallverständnis erweitern	Sachverhalt	Rücksprache mit Klient	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
6	Identifikation von Datenquellen, Triage	Herausfinden, welche Komponenten der IT-Infrastruktur zu untersuchen sind, schnelle Filterung von relevanten Datenquellen	Vorbereitung	Datenquellen sind nicht eindeutig, IT-Infrastruktur, Projektskizze, Erstaufnahme, Beweisfragenformulierung	Welche Teile der IT-Infrastruktur können oder sollen ausgewertet werden? Eventuell auch noch nach Erstauswertung	Dateien auf zu untersuchenden Datenquellen	Rücksprache mit Klient, intellektuelle Beurteilung	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
7	Sicherung, Imaging	Forensisch fachgerechte Sicherung von fallrelevanten Datenträgern, Imagen von diversen Objekten unter der Verwendung eines Hardwareschreibschutzes	Vorbereitung	Notwendige Soft- und Hardware für Sicherung vorhanden, Identifikation von Datenquellen, Nämlichkeit	möglichst Bitgenaue Kopie des zu untersuchenden Mediums erstellen, um die Originaldaten nicht zu verfälschen	Dateien auf zu untersuchenden Datenquellen	Imaging, logische Sicherung, halbphysische Sicherung, Cloning, RAW,...	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
8	Nämlichkeit	Überprüfung der Kopie auf Lesbarkeit und Überprüfung der Nämlichkeit des Auftrags	Vorbereitung	Erstaufnahme, Beweisfragenformulierung, Identifikation von Datenquellen	Klären, ob überhaupt mit der Arbeit angefangen werden kann	Imagekopie	Lesbarkeit mit geeignetem Tool überprüfen, Nämlichkeit intellektuell einschätzen	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
9	Hardwarekomponenten	Herausfinden, welche Hardwarekomponenten in der zu untersuchenden Datenquelle verbaut sind	Vorbereitung	Identifikation von Datenquellen	Zu Dokumentations- und Analysezwecken notieren, welche Hardwarekomponenten vorhanden sind	zu untersuchendes Objekt	intellektuelle Sichtung	Client, Handy, Tablet, Server, interne Festplatte, Netzwerk, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung

Abbildung 9: Teil 3 der Bausteintabelle, Bereich: Vorbereitung

Nummer	Name	Beschreibung	Bereich	Voraussetzung	Ziel	Artefakt	Methode	Objekt	Betriebssystem	Untersuchungsziel
12	Dateisystem	Herausfinden, um welches Dateisystem (FAT, ext, NTFS, DOS, HSF,...) es sich handelt, um angepasste Analysen durchzuführen	Aufbereitung	Sicherung	Dateisystem-bestimmung zur effizienteren Datenanalyse	Imagekopie	Dateisystem-Signatur mit geeignetem Tool suchen	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, CD/DVD, Kamera, Rekorder, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
13	Partitionierung	Herausfinden, welche und wie viele Partitionen das Dateisystem hat und wie sie angelegt sind, um angepasste Analysen durchzuführen (MBR, Laufwerke (logisch, virtuell), Swap-Partitionen, GPT, ...)	Aufbereitung	Sicherung	Partitionierungsbestimmung zur effizienteren Datenanalyse	Imagekopie	Image in geeignetem Tool daraufhin untersuchen	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, CD/DVD, Kamera, Rekorder, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
14	Betriebssystem	Herausfinden, wann welches Betriebssystem (Unix, Linux, BSD, MAC OS, Android, Blackberry OS, MS DOS, Win NT,...) installiert war/installiert wurde, um angepasste Analysen durchzuführen	Aufbereitung	Sicherung	Betriebssystembestimmung zur effizienteren Datenanalyse	Imagekopie	Image in geeignetem Tool daraufhin untersuchen	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, CD/DVD, Kamera, Rekorder, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
15	Rekosntruktion, Carving	Wiederherstellung gelöschter oder ehemalig existierender Dateien, auch aus dem Papierkorb, auch Rekonstruktion von virtuellen Maschinen oder RAIDS, beinhaltet Rekonstruktionsversuche für physisch beschädigte Objekte	Aufbereitung	gelöschte Dateien vermutlich vorhanden, ein Netzwerksystem muss rekonstruiert werden (RAID)	Untersuchung von gelöschten oder ehemalig existierenden Dateien möglich machen	Datenbestand, RAID, virtuelle Maschine	Rekonstruktion oder Carving mit geeignetem Tool	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
16	Systemabbilder	Überprüfen, ob Restore Points existent sind und das ganze System oder den Hauptspeicher mittels Schattenkopien o.ä. in einen früheren Zustand zurückführen	Aufbereitung	System muss oder soll, beispielsweise wegen Zerstörung, wiederhergestellt werden	Daten finden und wiederherstellen, die eventuell im aktuellen Rechnerzustand nicht mehr vorhanden sind	Restore Points, hilberfil.sys, Schattenkopien	intellektuelle Sichtung mittels geeignetem Tool	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, CD/DVD, Kamera, Rekorder, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
17	Wiederherstellung aus Backups	Überprüfen, ob es bereits gespeicherte Backups gibt, die man forensisch untersuchen könnte oder ob es Backups gibt, die man im Fall eines Incidents wieder einspielen könnte	Aufbereitung	System muss oder soll, beispielsweise wegen Zerstörung, wiederhergestellt werden	Daten finden und wiederherstellen, die eventuell im aktuellen Rechnerzustand nicht mehr vorhanden sind	Backups	Einbinden mit geeignetem Tool und intellektuelle Sichtung	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
18	Entschlüsselung	Entschlüsseln vorhandener Datenquellen, um sie lesbar zu machen, gilt auch für betroffene Systeme bei Incidents, Überwinden von Zugangshürden, PIN-Code-Eingaben, etc.	Aufbereitung	Verschlüsselung vorhanden, Passwortdokumente	Image lesbar machen	Imagekopie	Vorhandenen Schlüssel auf das Image anwenden	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
19	Filterung, Datenreduktion	Die Datenmenge nach beispielsweise der relevanten Zeitspanne filtern	Aufbereitung	Untersuchungsfragen klar	Die vorhandene Datenmenge reduzieren	Datenbestand	intellektuelle Festlegung des geeigneten Zeitraums, Filterung mittels geeignetem Tool	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
20	Formatkonvertierung	Ein Imageformat in ein anderes umwandeln	Aufbereitung	Probleme bezüglich der Lesbarkeit von anderen Dateiformaten	Die Kopie für etwaige forensische Software zugänglich machen	Imagekopie	Konvertierung mittels geeignetem Tool	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung

Abbildung 10: Teil 4 der Bausteintabelle, Bereich: Aufbereitung

Nummer	Name	Beschreibung	Bereich	Voraussetzung	Ziel	Artefakt	Methode	Objekt	Betriebssystem	Untersuchungsziel
21	Suchindex	Erstellung eines Indexes aus lesbaren Zeichen, zur Beschleunigung von Suchvorgängen (E-Mail-Adressen, Telefonnummern, fallrelevante Wörter, Namen,…)	Auswertung	Großer Fall, e-Discovery-Fall, Klarheit, wonach ungefähr gesucht wird	Herausfiltern fallrelevanter Daten ermöglichen, zu durchsuchende Datenmenge reduzieren	Dateien auf zu untersuchenden Datenquellen	Suchbegriffe auflisten	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
22	Erstsichtung	Erstsichtung des Dateisystems auf relevante Datenbereiche und zeitlich passende, auffällige Ereignisse	Auswertung	Entschlüsselung, falls verschlüsselt	Einen Überblick über bisherige Ereignisse, Datenbestände und Probleme bekommen	Imagekopie	intellektuell einen Überblick schaffen	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
23	Live-Forensik	Sammeln erster Erkenntnisse über Sachverhalte des Falls mittels Untersuchungen am laufenden System, Untersuchung von flüchtigem Speicher, Vorgängen des laufenden Systems…	Auswertung	Notwendigkeit von Incident Response oder „erster Hilfe" vor Ort am eingeschalteten System	Erkenntnisse zu Vorfällen auf kompromittierten Systemen sammeln, ohne flüchtige Daten durch Shutdown zu vernichten	kompromittiertes System	intellektuelle Sichtung	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
24	laufende Prozesse	Das zu untersuchende Medium auf laufende Prozesse hin untersuchen, flüchtige Daten sichern, bevor die Stromzufuhr entfernt wird	Auswertung	Live-forensische Untersuchung	Untersuchung laufender Prozesse, um mögliche beispielsweise schädliche Prozesse herauszufiltern	kompromittiertes System, Task Manager, Systemüberwachung	intellektuelle Sichtung und Sicherung mit geeignetem Tool	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
25	Arbeitsspeicher	Untersuchung von flüchtigen Daten im RAM auf dem Zielsystem beispielsweise von laufenden Prozessen und Diensten, Netzwerkverbindungen, Passwörtern,…	Auswertung	Live-forensische Untersuchung	Auswertung des Arbeitsspeichers mittels Live-Forensik	pagefile.sys, hiberfil.sys, Task Manager, Kernel Level Applications	intellektuelle Sichtung und Sicherung mit geeignetem Tool	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
26	Post-mortem-Analyse	Untersuchung, die auf Datenquellkopien durchgeführt wird, Gewährleistung des Originalzustands	Auswertung	Sicherung	intellektuelle Durchsicht der Festplattenkopie, um fallrelevante Daten zu extrahieren	Datenbestand	intellektuelle Untersuchung	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
27	Malwareprüfung	Überprüfung des Systems auf Malware, sofern Incidents vorhanden	Auswertung	Malwarebefall vermutet	Weitere Ausbreitung von Malware auf dem Zielsystem verhindern, analysieren ob akute Bedrohung immer noch besteht	kompromittiertes System	Virenscan per externem USB-Stick, installierter Software	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
28	User	Datenquellen oder Artefakte auf fallrelevante Daten untersuchen (Rechte, angemeldete User, Urheberrechtsverletzungen, Login Daten/Passwörter, Wasserzeichen,….)	Auswertung	Ursachenforschung	Fallrelevante Userdaten extrahieren	Text-, Bild-, Audio-, Videodateien	Dateien mit geeignetem Tool filtern und intellektuell auswerten	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, CD/DVD, Konsole	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
29	Software	Untersuchung des Systems auf Software im Bezug auf den zu untersuchenden Sachverhalt. Klärung der Frage, welche Systeme beispielsweise im Autostart laufen, ob es dualuse-Software gibt oder versteckte Prozesse	Auswertung	Ursachenforschung	Herausfinden, ob auf dem zu untersuchenden Medium fallrelevante Software existiert	Datenbestand	intellektuelle Sichtung	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, CD/DVD, Konsole	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung

Abbildung 11: Teil 5 der Bausteintabelle, Bereich: Auswertung

Abbildung 12: Teil 6 der Bausteintabelle, Bereich: Auswertung

30	externe Geräte	Klärung der Frage, ob externe Geräte und Datenträger angeschlossen wurden (USB-Sticks, Drucker, Handys, Festplatten, Kameras,...), um Daten zu kopieren, betrifft auch Fremdgeräte im Netzwerk	Auswertung	Datentransfer vermutet	Herausfinden, ob externe Datenträger angeschlossen und beispielsweise Daten transferiert wurden	Logfiles	Logfiles mittels geeignetem Tool untersuchen	Client, Handy, Tablet, Server, interne Festplatte, Netzwerk, Drucker, Kopiergerät, Scanner, Receiver, Konsole, Wiedergabegerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
31	Sitzungsdaten	Untersuchung von Sitzungsdaten, die von Usern, Benutzern, Betriebssystemen oder anderen Anwendungen erzeugt wurden	Auswertung	Ursachenforschung	Klärung der Frage, wann Sitzungen jeglicher Art stattfanden und was während der Sitzungen passierte	Datenbestand, Logfiles, *.plist-Files, Registry-Files	intellektuelle Sichtung und Sicherung mit geeignetem Tool	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, CD/DVD, Konsole	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
32	Kommunikationsprotokolldaten	Das zu untersuchende Medium auf fallrelevante Kommunikationsprotokolldaten, z.B. Netzwerkverbindungen untersuchen, bei Protokolldaten, betrifft auch die Auswertung von Instant-Massaging-Dateien	Auswertung	Ursachenforschung	Zeitliche Einordnung von Ereignissen, mehr über Ablauf von Ereignissen erfahren	ARP-Cache, Routingtabelle, Logfiles, APP- und Software Daten	intellektuelle Sichtung und Sicherung mit geeignetem Tool	Client, Handy, Tablet, Server, interne Festplatte, Speicherkarte, Telefon, Konsole, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
33	Systemzeit	Klärung der Frage, welche Systemzeit für die auf dem Speichermedium enthaltenen Dateien vorliegt	Auswertung	Ursachenforschung	Zeitliche Einordnung von Ereignissen, auffällige Aktivitäten ermitteln, mögliche Manipulationen feststellen	BIOS, MAC-Zeitstempel	intellektuelle Sichtung	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
34	Systemaktivitäten, Eventlogs	Untersuchung von Windows Eventlogs und anderen Systemaktivitäten auf fallrelevante Aktivitäten und Auffälligkeiten	Auswertung	Ursachenforschung	Zeitliche Einordnung von Ereignissen, auffällige Aktivitäten ermitteln	*.evt-Files, security- und appdata	Dateien mit geeignetem Tool filtern und intellektuell auswerten	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
35	Registry	Untersuchen der Windows Registry und Konfigurationsdateien zur Auswertung von Nutzeraktivitäten	Auswertung	Ursachenforschung	zeitliche Einordnung fallrelevanter Daten, Überprüfung von Nutzeraktivitäten	SAM, SECURITY, SYSTEM, NTUSER.DAT, USRCLASS.DAT, Hardware, Treiber, geöffnete Dateien, ...	intellektuelle Durchsicht, Auswahl von geeigneten Tools zur Filterung, flüchtige Speicherung mit geeigneten Tools	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, CD/DVD, Konsole	Windows, Windows Phone	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
36	Konfigurationsdateien	Untersuchen, welche Konfigurationen auf dem zu untersuchenden System eingestellt sind	Auswertung	Ursachenforschung	Aktive Konfiguration von beispielsweise dem Netzwerk und dessen Loggings	*.plist-Files, Registry-Files, syslog-Files	Dateien mit geeignetem Tool filtern und intellektuell auswerten	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung

39	Metadaten	Auswertung von möglicherweise fallrelevanten Dateiinformationen zuzüglich zur MAC-Time, Rücksichtnahme auf beispielsweise Autoren von Textdateien	Auswertung	interessante, prüfbare Dateien vorhanden	jegliche Informationen für interessante Dateien erhalten	Text-, Bild-, Audio-, Videodateien, prefetch-Dateien	Dateien mit geeignetem Tool filtern und intellektuell auswerten	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
40	Erweiterte Attribute	Untersuchung des ADS im Hinblick auf eventuell versteckte Daten	Auswertung	Verdacht auf versteckte Dateien	Klärung der Frage, ob Dateien in den ADS' versteckt werden sollten	Alternate Data Stream (NTFS/MFT), Extended Attributes	Mittels geegnetem Tool nach Dateifragmenten suchen	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
41	Fileslack-Analyse	Suche nach noch existierenden relevanten Restdaten und Dateifragmenten oder gelöscht geglaubten Inhalten	Auswertung	Prüfung auf Restexistenz relevanter Dateien notwendig	Finden gelöscht geglaubter Inhalte, Restdaten und Dateifragmenten	RAM-, Drive-, MFT-, Partition-Slacks	Datenbestand mittels geeignetem Tool untersuchen	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
42	Internetaktivität	Klärung der Frage, welche fallrelevanten Internetaktivitäten es gibt und in wie fern auf dieses zugegriffen werden kann (Struktur), Browserdaten (Internet Explorer, Google Chrome, …)	Auswertung	Ursachenforschung	Herausfinden, ob es fallrelevante Internetaktivitäten gab	Logfiles, RDP, Cookies, , Browser, TempäFiles, Cache, Firewall, Apache	Logfiles mittels geeignetem Tool untersuchen	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
43	E-Mail-Client, Webmailer	Auswertung fallrelevanter E-Mails mittels Suche nach Stichworten, Untersuchung verschiedener Mailclients, beispielsweise MS Outlook	Auswertung	Interessanter Kontakt zwischen zwei oder mehr Personen wird vermutet	Untersuchung etwaiger extrahier- und lesbarer fallrelevanter E-Mails	Protokolldateien, Temporary Files, *.pst, pagefile.sys	Dateien mit geeignetem Tool filtern und intellektuell auswerten	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
44	Plausibilisierung, Zeitstempelanalyse	Auswertung von Zeitstempeln und Suche nach Zeitstempeln in relevanten Zeiträumen von relevanten Dateien, Anwendungen und diverser anderer Betriebssystemartefakte, insgesamt intellektuelle Einordnung relevanter Beweismittel und Plausibilisierung derselben	Auswertung	Ursachenforschung	Zeitliche Einordnung fallrelevanter Daten, Überprüfung derer Wichtigkeit, Verstehen zeitlicher Zusammenhänge	gefilterte, extrahierte, als relevant eingestufte Daten	intellektuell Zusammenhänge herstellen	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
45	Anrufprotokolle	Letzte getätigte und empfangene Anrufe des Nutzers nachvollziehen	Auswertung	Interessanter Kontakt zwischen zwei oder mehr Personen wird vermutet	Feststellen, ob es im relevanten Zeitraum relevante getätigte oder empfangene Anrufe gab	Anrufprotokoll	Dateien mit geeignetem Tool filtern und intellektuell auswerten	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, Telefon, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Android, iOS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
46	SMS/MMS	SMS/MMS des Nutzers auf fallrelevante Informationen untersuchen	Auswertung	Interessanter Kontakt zwischen zwei oder mehr Personen wird vermutet	Feststellen, ob es fallrelevante gesendete oder empfangene SMS/MMS gab	SMS/MMS-Ordner	Dateien mit geeignetem Tool filtern und intellektuell auswerten	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, Telefon, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Android, iOS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung

Abbildung 13: Teil 7 der Bausteintabelle, Bereich: Auswertung

47	Audio-, Video- und Bilddateien	Untersuchung von Dateiinhalten	Auswertung	Bestimmte Dateien werden gesucht	Feststellen, ob Dateien zum Beisipiel Illegale Inhalte aufweisen, auch relevant bei der Suche nach Passwörtern	Audio-, Bild- und Videodateien	Dateien mit geeignetem Tool filtern und intellektuell auswerten	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
49	Täterprofilanalyse	Herausfinden, um was für einen Täter es sich handelt, falls ein Täter vermutet wird, was er für Beweggründe haben könnte, Untersuchung von Internetaktivitäten, sozialen Netzwerken, Foren, Postings,....	Auswertung	Es gibt Hinweise auf einen Täter und Spuren, anhand welcher man ihn analysieren kann	Täteridentifikation	Internetnutzung, soziale Netzwerkaktivitäten, Nutzeraktivitäten	intellektuelles Zusammenführen und analysieren terrelevanter Daten	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
53	Telefonanlagen	Untersuchung von Telefonanalagen auf bestimmte Einstellungen oder gar Abhöreinrichtungen	Auswertung	Vermutung auf Fehlkonfiguration oder Abhöreinrichtungen	IT-forensische Untersuchung von Telefonanlagen auf ungewöhnliche Einstellungen	Telekommunikation	intellektuelle Sichtung	Telefon		unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
54	Schadensausmaß	Bestimmung des Schadensausmaßes bei IT-Sicherheitsvorfällen	Auswertung	Opfer erleidet Datenverlust	Schadensausmaß für Unternehmen schätzen, um einen Schweregrad festzustellen	Malware, Netzwerk	intellektuelle Beurteilung anhand von beschädigten Daten(mengen)	Netzwerk, Client, Server, Handy, Tablet, interne Festplatte	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
55	Software-/Codevergleich	Bestimmung verschiedener Versionsstände von Software oder Code	Auswertung	Verdacht auf Diebstahl geistigen Eigentums	Untersuchung verschiedener Programmsoftware	Code	intellektuelle Bewertung von Softwarecode	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
56	Schädlingsidentifikation	Herausfinden, wodurch das System befallen wurde	Auswertung	Malware vorhanden	Herausfinden, welche Malware auf den Systemen zugeschlagen hat, um mögliche Einfallsmöglichkeiten zu überprüfen, oder Möglichkeiten zu finden, die Dateien wieder zu entschlüsseln	Malware, Netzwerk	Suche in Virusdatenbanken, intellektuelle Vergleiche, intellektuelle Bewertung	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	Malware

Abbildung 14: Teil 8 der Bausteintabelle, Bereich: Auswertung

57	Verschlüsselungsablauf	Analysieren, wie die Verschlüsselung abgelaufen ist	Auswertung	Malware oder anderweitige Verschlüsselungssoftware vorhanden	Herausfinden, welche Teile der IT betroffen sind und in welcher Reihenfolge sie betroffen wurden, um mögliche Einfallstore einzugrenzen	Malware, Netzwerk	Sichtung der betroffenen IT-Systeme, intellektuelle Beurteilung	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, USB-Stick, Speicherkarte, Konsole, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	Malware	
59	Cloud-Speicher	prüfen, ob es Cloudspeichermöglichkeiten gibt und ob sich dort eventuell relevante Daten befinden	Auswertung	Der Anspruch ist eine vollständige Datenerhebung	Herausfinden, ob es Cloudspeichermöglichkeiten gibt, um alle möglichen Datenspeicherorte zu berücksichtigen	Cloudspeicher	Erfragen von möglichen Cloudspeichern, scannen nach Verbindungen zu Cloudspeichern mit geeigneten Tools, intellektuelle Auswertung	Client, Handy, Tablet, Server, interne Festplatte, Netzwerk, Konsole, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung	
61	Finanzdaten	Anforderung und Auswertung von Finanzdaten eines Verdächtigen oder eines Opfers, Einsicht in SAP/ERP-Systeme	Auswertung	Die Situation lässt die Überprüfung dieser Daten zu	Auswertung von Finanzdaten, um auffällige finanzielle Transaktionen oder Situationen zu erkennen und zu analysieren	Kontoauszüge, online-Banking-Daten, Scheckhefte, Kassenzettel,...	Zugriff auf entsprechende Dokumente erwirken und diese intellektuell auswerten	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	Betrug, Erpressung	
62	Lokalisation	Lokalisation eines potentiellen Täters durch Rückverfolgen seiner IP-Adresse oder seiner GPS-Koordinaten	Auswertung	Die IP-Adresse oder die GPS-Koordinaten sind nach Deutschland zurückzuverfolgen und nicht gefälscht	Zurückverfolgen von Standortmarkern, um einen möglichen Täter zu lokalisieren	GPS-Koordinaten	Ortung von Standortmarkern mittels geeigneter Tools	Client, Handy, Tablet, Server, interne Festplatte, Receiver, Konsole, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung	

Abbildung 15: Teil 9 der Bausteintabelle, Bereich: Auswertung

Nummer	Name	Beschreibung	Bereich	Voraussetzung	Ziel	Artefakt	Methode	Objekt	Betriebssystem	Untersuchungsziel
48	Sicherheitslücken, Fernzugriffsmöglichkeiten	Suche nach Sicherheitslücken im Netzwerk der Firma mit beispielsweise einem Sicherheitsvorfall, Überprüfung auf aktuelle Patch- und Konfigurationsstände, Untersuchung von Remotezugriffsmöglichkeiten, Passwortweitergaben, Zugriffsmöglichkeiten auf Clients und Server generell, Datenabflüsse, Einstellungsänderungen, Trojaner, Rootkits, Sniffer,...	IT-Sicherheit	Sicherheitsvorfall	Ausmachen von Sicherheitslücken, wie kann auf das System von außen und innen zugegriffen werden?	eventlogs, Nutzungsrechte, Sitzungsdaten, virtuelle Maschinen...	Sicherheitslücken intellektuell ausmachen und Angriffswege nachvollziehen	Client, Handy, Tablet, Server, externe Festplatte, interne Festplatte, Netzwerk, USB-Stick, Speicherkarte, CD/DVD, Drucker, Kopiergerät, Scanner, Werkzeugmaschine, Telefon, Kamera, Rekorder, Receiver, Konsole, Wiedergabegerät, Haushaltsgerät, Fahrzeugelektronik	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung
51	„Fallen" für Systemeindringlinge	Hacker im System durch vorgegebenes Netzwerk fangen und dessen Aktivitäten nachvollziehen und aufdecken, Spiegelung des Netzwerkverkehrs, Honeypots, nachladbare Pixel	IT-Sicherheit	merkwürdige Netzwerkaktivitäten, Vermutung auf Systemeindringling	Unberechtigte Nutzer in einem IT-System feststellen und aufhalten	Netzwerkverkehr	Nachstellung von Szenarien und intellektuelle Auswertung der daraus resultierenden Ergebnisse	Netzwerk	Windows, Linux, MAC OS, Android, i OS, Windows Phone, BlackBerry	unzulässige Nutzung, Datenabfluss, Malware, Betrug, Besitz illegaler Dateien, Erpressung, Identitätsdiebstahl, Diebstahl geistigen Eigentums, Belästigung

Abbildung 16: Teil 10 der Bausteintabelle, Bereich: IT-Sicherheit

3.7 Darstellung für einen Walkthrough geeigneter Vorfallsszenarien aus Literatur und Praxis

Konkrete Untersuchungsaufträge könnten laut „Computer Forensics Evidence Collection & Preservation“ von Course Technology [24], S. 34 in etwa wie folgt aussehen:

- Untersuchung auf Betrug durch Manipulation von Computeraufzeichnungen
- Untersuchung auf Vorschriftsverletzungen
- Untersuchung eines Systems auf absichtliche Umgehung von Zugangshürden
- Unberechtigter Zugriff auf Software und unerlaubte Änderung dieser
- Untersuchung eines Systems auf mutmaßlichen Diebstahl geistigen Eigentums
- Industriespionage durch Zugang zu oder Diebstahl von Computermaterialien
- Identitätsdiebstahl durch betrügerische Computertransaktionen
- Untersuchung eines Computerssystems wegen Verdachts auf Herstellung oder Verbreitung von Computerviren oder Würmern
- Untersuchung eines Computersystems auf Finanzbetrug, bei dem immer wieder in kleinen Mengen Geld gestohlen wird
- Untersuchung eines Computersystems auf den Besitz illegaler Daten

Konkrete Fallbeispiele aus dem DigiTrace-Unternehmensalltag:

- Systemeinbrüche
- Unterschlagungen
- Missbrauch von IT-Systemen und -Anwendungen (IT misuse)
- Betrugsfälle
- Erpressung
- IT-Sabotage

- Malware
- Datenabfluss

3.8 Zuordnung zwischen Anwendungsfällen aus der Praxis und Bausteinen

In diesem Abschnitt werden die nunmehr im Modell verfügbaren Bausteine in Beziehung zu einzelnen Bereichen IT-forensischer Untersuchungen und ausgewählten Anwendungsfällen gesetzt. Die Beziehungen zwischen Untersuchungsfragen und -bausteinen wurden vor allen Dingen durch gezielte Abgleiche von Untersuchungsplänen, die für ein bestimmtes Problem erstellt wurden, und durch das mit Herrn Sigel geführte Interview zu geeigneten Untersuchungsschritten für ein bestimmtes Problem hergestellt.

Allgemeine Bausteine, um mit einer forensischen Untersuchung zu beginnen oder fortfahren zu können, die nicht in direktem Zusammenhang mit der auswertenden Untersuchung an sich stehen, sind:

„Erstaufnahme/Beweisfragenformulierung“, „Projektskizze“, „IT-Infrastruktur“, „Personennetzwerk“, „Verflechtungsgrafik“, „Identifikation von Datenquellen/Triage“, „Sicherung/ Imaging“, „Hintergrundrecherchen“, „Beratung“, „Nämlichkeit“, „Erstsichtung“, „Täterprofilanalyse“, „Audio-, Video- und Bilddateien/Passwortdateien/Finanzdaten“, „Experimente“, „Softwareentwicklung“, „Systemaktivitäten“, „Eventlogs und Zeitstempelanalyse“, „Plausibilisierung“

Bausteine aus den Bereichen „Auswertung“ und „Aufbereitung“, die jede post-mortem-Untersuchung beinhaltet:

„Hardwarekomponenten“, „Dateisystem“, „Partitionierung“, „Betriebssystem“, „Filterung/Datenreduktion“, „Formatkonvertierung“, „User“, „Sitzungsdaten“, „Systemzeit“, „Zeitstempelanalyse/ Plausibilisierung“

Bausteine die wichtig sind, falls man das System wiederherstellen will (Sicherheitsvorfälle, Löschung von Dateien):

„Carving“, „Systemabbilder“, „ADS“, „Slack“, „E-Mail-Client“, „(Internetaktivität)“, „Cloudspeicher“

Bausteine die vor allem bei Untersuchungen von Incident Response-Fällen bezüglich Malware wichtig sind:

„Live-Forensik“, „laufende Prozesse“, „Arbeitsspeicher“, „Malwareprüfung“, „Schädlingsidentifikation“, „Nachvollziehen des Verschlüsselungsablaufs“, „Hintergrundrecherchen“, „Sicherheitslücken/Fernzugriffsmöglichkeiten“, „Software“, „externe Geräte“, „Kommunikationsprotokolldaten“, „Systemaktivitäten/Eventlogs“, „Registry“, „Konfigurationsdateien“, „Internetaktivität/Cloudspeicher“, „E-Mail-Client/Webmailer“, „Anrufprotokolle/SMS/MMS“, „Carving/Rekonstruktion“, „Netzwerksystem spiegeln“, „Sicherheitslücken/Fernzugriffsmöglichkeiten“, „Schädlingsidentifikation“, „Verschlüsselungsablauf“, „Telefonanlagen“, „Bestimmung des Schadensausmaßes“

Bausteine die für Incident Response wichtig sind, wenn ein aktiver Eindringling im System vermutet wird:

„Software“, „Erstellung eines Honeypots“, „Einrichtung von Zugangshürden“, „Erstellung von nachladbaren Pixeln (IP-Tracking)“

Bausteine die insbesondere für e-Discovery wichtig sind:

„Suchindex“, „E-Mail-Client/Webmailer“

Bausteine die wichtig sind, wenn es um Datenfälschung und Besitz illegaler oder illegitimer Dateien geht:

„Besondere Überprüfung von Dokumenten“, „Audio- Video- und Bilddateien“, „Software“, „Metadaten“, „ADS“, „Slack“, „Internetaktivität (Profile, Postings, Favoriten)“, „Aktivität in sozialen Netzwerken“, „E-Mail-Client“, „Cloudspeicher“, „Hashwertvergleiche“

Bausteine die wichtig sind, wenn es um Stalking oder sonstige Belästigungen geht:

„Anrufprotokolle“, „SMS/MMS“, „Kommunikationsprotokolldaten/Datenanforderung“, „Internetaktivitäten/Cloudspeicher“, „Täterprofilanalyse“, „Überprüfung von Telefonanlagen“

Bausteine die wichtig sind, wenn es um Betrugsfälle oder Finanzbetrug geht:

„Finanzdaten“, „Prüfung von Dokumenten und deren Metadaten“, „Slack“, „ADS“, „E-Mail-Client/Webmailer“, „Kommunikationsprotokolldaten“, „Internetaktivität/Cloudspeicher, Audio-, Video- und Bilddateien“, „Passwortdateien“, „Finanzdaten“, „Überprüfung von Telefonanlagen“

Bausteine die wichtig sind, wenn es um Diebstahl geistigen Eigentums (Softwarediebstahl) geht:

„Software- /Codevergleich“, „Versionsüberprüfung“

3.9 Überprüfung der Abdeckung (Walkthrough)

In diesem Abschnitt wird das entwickelte Modell mit den Bausteinen auf zwei ausgewählte Untersuchungsszenarien angewendet, um im Rahmen eines Durchlaufs (Walkthroughs) qualitativ zu überprüfen, wie vollständig oder geeignet die Abdeckung für diese beiden Fälle ist. Es handelt sich um die beiden Anwendungsszenarien „Malware auf einem Client mit Windows als Betriebssystem“ und „Datenabfluss auf einem Client mit Windows als Betriebssystem“, die sich auf die zuvor vorgestellten identifizierten Anwendungsszenarien beziehen und ausgewählt wurden, da diese Untersuchungen große Praxisrelevanz besitzen. Hierzu wurden die Tabellen in der Datenbank von „MySQL“ aktualisiert und die Datenbankabfragen entsprechend angepasst.

Alle Relationstabellen der Datenbank aus dem Praxisprojekt wurden angepasst.

Zum Vergleich und um an das Praxisprojekt anschließen zu können, nachfolgend die Abfrage aus 3.5 „Client, Linux, Datenabfluss“:

```
use methodenbausteine;

select bausteine.BauName, bausteine.Bname, objekte.ObjName, be-
triebssysteme.BSName, untersuchungsziel.ZielName

from bausteine, objekte, betriebssysteme, untersuchungsziel,
bau_obj, bau_bs, bau_ziel, bs_obj

 where     bausteine.BauIndex = bau_obj.BauIndex
 And  bausteine.BauIndex = bau_bs.BauIndex
 And  Detektorbaustein = bau_ziel.BauIndex
 And  bau_obj.BauIndex = bau_bs.BauIndex
 And  bau_obj.BauIndex = bau_ziel.BauIndex
 And  bau_bs.BauIndex = bau_ziel.BauIndex
 And  objekte.ObjIndex = bs_obj.ObjIndex
 And  objekte.ObjIndex = bau_obj.ObjIndex
 And  bs_obj.ObjIndex = bau_obj.ObjIndex
```

```
And betriebssysteme.BSIndex = bau_bs.BSIndex
And betriebssysteme.BSIndex = bs_obj.BSIndex
And bau_bs.BSIndex = bs_obj.BSIndex
And untersuchungsziel.ZielIndex = bau_ziel.ZielIndex
And
       objekte.ObjName = "Client"
       And
       betriebssysteme.BSName = "Linux"
       And
       untersuchungsziel.ZielName = "Datenabfluss";
```

BauName	Bname	ObjName	BSName	ZielName
Sicherung, Imaging	Vorbereitung	Client	Linux	Datenabfluss
Nämlichkeit	Vorbereitung	Client	Linux	Datenabfluss
Hardwarekomponenten	Vorbereitung	Client	Linux	Datenabfluss
Sicherheitslücken, Fernzugriffsmöglichkeiten	IT-Sicherheit	Client	Linux	Datenabfluss
Suchindex	Auswertung	Client	Linux	Datenabfluss
Erstsichtung	Auswertung	Client	Linux	Datenabfluss
Live-Forensik	Auswertung	Client	Linux	Datenabfluss
laufende Prozesse	Auswertung	Client	Linux	Datenabfluss
Arbeitsspeicher	Auswertung	Client	Linux	Datenabfluss
Post-mortem-Analyse	Auswertung	Client	Linux	Datenabfluss
Malwareprüfung	Auswertung	Client	Linux	Datenabfluss
User	Auswertung	Client	Linux	Datenabfluss
Software	Auswertung	Client	Linux	Datenabfluss
externe Geräte	Auswertung	Client	Linux	Datenabfluss
Sitzungsdaten	Auswertung	Client	Linux	Datenabfluss
Kommunikationsprotokolldaten	Auswertung	Client	Linux	Datenabfluss
Systemzeit	Auswertung	Client	Linux	Datenabfluss
Systemaktivitäten, Eventlogs	Auswertung	Client	Linux	Datenabfluss
Konfigurationsdateien	Auswertung	Client	Linux	Datenabfluss
Stichwortsuche	Auswertung	Client	Linux	Datenabfluss
Dateisignaturprüfung	Auswertung	Client	Linux	Datenabfluss
Metadaten	Auswertung	Client	Linux	Datenabfluss
Erweiterte Attribute	Auswertung	Client	Linux	Datenabfluss
Fileslack-Analyse	Auswertung	Client	Linux	Datenabfluss
Internetaktivität	Auswertung	Client	Linux	Datenabfluss
E-Mail-Client, Webmailer	Auswertung	Client	Linux	Datenabfluss
Plausibilisierung, Zeitstempelanalyse	Auswertung	Client	Linux	Datenabfluss
Audio-, Video- und Bilddateien	Auswertung	Client	Linux	Datenabfluss
Täterprofilanalyse	Auswertung	Client	Linux	Datenabfluss
Schadensausmaß	Auswertung	Client	Linux	Datenabfluss
Software-/Codevergleich	Auswertung	Client	Linux	Datenabfluss
Cloud-Speicher	Auswertung	Client	Linux	Datenabfluss
Lokalisation	Auswertung	Client	Linux	Datenabfluss
Dateisystem	Aufbereitung	Client	Linux	Datenabfluss
Partitionierung	Aufbereitung	Client	Linux	Datenabfluss
Betriebssystem	Aufbereitung	Client	Linux	Datenabfluss
Rekonstruktion, Carving	Aufbereitung	Client	Linux	Datenabfluss
Systemabbilder	Aufbereitung	Client	Linux	Datenabfluss
Wiederherstellung aus Backups	Aufbereitung	Client	Linux	Datenabfluss
Entschlüsselung	Aufbereitung	Client	Linux	Datenabfluss
Filterung, Datenreduktion	Aufbereitung	Client	Linux	Datenabfluss
Formatkonvertierung	Aufbereitung	Client	Linux	Datenabfluss
Hashwertvergleich	Allgemeines	Client	Linux	Datenabfluss
Hintergrundrecherchen	Allgemeines	Client	Linux	Datenabfluss

Abbildung 17: Vergleichsabbildung der Abfrage aus 3.5 „Client, Linux, Datenabfluss“

Bereits im Praxisprojekt wurde ein Untersuchungsplan nachgebaut, der in der Praxis wie folgt aussah:

1. Erstaufnahme von Informationen zum Sachverhalt (zwei Telefonate)
2. Identifikation des Laptops, Ausbau und Identifikation der SSD, Dokumentation
3. IT-forensische Sicherung der Daten auf der SSD am Hardware-Schreibschutz
4. Recherchen zur Malware Gootkit-CNC, zu dateiloser Malware und zum Angler Exploit Kit, samt Ableitung und Überprüfung möglicher Erkennungsmerkmale
5. Mit X-Ways-Forensics: Überprüfung des Images auf Lesbarkeit, Nämlichkeitsdentifikation, Erstsichtung auf Dateien im relevanten Zeitraum und passende auffällige Ereignisse
6. Untersuchung der Windows-Registry mit RegRipper und zeitlich mit egtimeline auf auffällige Veränderungen und Ereignisse im Verdachtszeitraum
7. Untersuchung von Windows-Eventlogs auf auffällige Ereignisse im Verdachts zeitraum
8. Denkbarer Infektionsweg Web: Untersuchung auf Web-Artefakte für die Browser Internet Explorer und Firefox
9. Denkbarer Infektionsweg USB: Untersuchung auf USB-Ereignisse, die im Zusammenhang mit infizierten externen Datenträgern stehen könnten
10. Wiederherstellung gelöschter bzw. früher existierender Dateien
11. Erstellung und Abgleich mittels Prüfsummen
12. Stichwortsuche im Image nach einschlägigen Zeichenketten
13. Scans auf Malware
14. Analyse Hauptspeicher-ähnlicher Artefakte aus dem Image
15. Post-mortem-Untersuchungen eines gebooteten Clones des Images auf Malware

Die Datenbankabfrage für diese Untersuchung sieht wie folgt aus:

```
use methodenbausteine;

select bausteine.BauName, bausteine.Bname, objekte.ObjName, be-
triebssysteme.BSName, untersuchungsziel.ZielName

from bausteine, objekte, betriebssysteme, untersuchungsziel,
bau_obj, bau_bs, bau_ziel, bs_obj

 where     bausteine.BauIndex = bau_obj.BauIndex
 And bausteine.BauIndex = bau_bs.BauIndex
 And bausteine.BauIndex = bau_ziel.BauIndex
 And bau_obj.BauIndex = bau_bs.BauIndex
 And bau_obj.BauIndex = bau_ziel.BauIndex
 And bau_bs.BauIndex = bau_ziel.BauIndex
 And objekte.ObjIndex = bs_obj.ObjIndex
 And objekte.ObjIndex = bau_obj.ObjIndex
 And bs_obj.ObjIndex = bau_obj.ObjIndex
 And betriebssysteme.BSIndex = bau_bs.BSIndex
 And betriebssysteme.BSIndex = bs_obj.BSIndex
 And bau_bs.BSIndex = bs_obj.BSIndex
 And untersuchungsziel.ZielIndex = bau_ziel.ZielIndex
 And
        objekte.ObjName = "Client"
        And
        betriebssysteme.BSName = "Windows"
        And
        untersuchungsziel.ZielName = "Malware";
```

und liefert folgendes Ergebnis:

BauName	Bname	ObjName	BSName	ZielName
Hashwertvergleich	Allgemeines	Client	Windows	Malware
Hintergrundrecherchen	Allgemeines	Client	Windows	Malware
Experimente	Allgemeines	Client	Windows	Malware
Softwareentwicklung	Allgemeines	Client	Windows	Malware
Datenanforderung	Allgemeines	Client	Windows	Malware
Dateisystem	Aufbereitung	Client	Windows	Malware
Partitionierung	Aufbereitung	Client	Windows	Malware
Betriebssystem	Aufbereitung	Client	Windows	Malware
Rekonstruktion, Carving	Aufbereitung	Client	Windows	Malware
Systemabbilder	Aufbereitung	Client	Windows	Malware
Wiederherstellung aus Backups	Aufbereitung	Client	Windows	Malware
Entschlüsselung	Aufbereitung	Client	Windows	Malware
Filterung, Datenreduktion	Aufbereitung	Client	Windows	Malware
Formatkonvertierung	Aufbereitung	Client	Windows	Malware
Suchindex	Auswertung	Client	Windows	Malware
Erstsichtung	Auswertung	Client	Windows	Malware
Live-Forensik	Auswertung	Client	Windows	Malware
laufende Prozesse	Auswertung	Client	Windows	Malware
Arbeitsspeicher	Auswertung	Client	Windows	Malware
Post-mortem-Analyse	Auswertung	Client	Windows	Malware
Malwareprüfung	Auswertung	Client	Windows	Malware
User	Auswertung	Client	Windows	Malware
Software	Auswertung	Client	Windows	Malware
externe Geräte	Auswertung	Client	Windows	Malware
Sitzungsdaten	Auswertung	Client	Windows	Malware
Kommunikationsprotokolldaten	Auswertung	Client	Windows	Malware
Systemzeit	Auswertung	Client	Windows	Malware
Systemaktivitäten, Eventlogs	Auswertung	Client	Windows	Malware
Registry	Auswertung	Client	Windows	Malware
Konfigurationsdateien	Auswertung	Client	Windows	Malware
Stichwortsuche	Auswertung	Client	Windows	Malware
Dateisignaturprüfung	Auswertung	Client	Windows	Malware
Metadaten	Auswertung	Client	Windows	Malware
Erweiterte Attribute	Auswertung	Client	Windows	Malware
Fileslack-Analyse	Auswertung	Client	Windows	Malware
Internetaktivität	Auswertung	Client	Windows	Malware
E-Mail-Client, Webmailer	Auswertung	Client	Windows	Malware
Plausibilisierung, Zeitstempelanalyse	Auswertung	Client	Windows	Malware
Audio-, Video- und Bilddateien	Auswertung	Client	Windows	Malware
Täterprofilanalyse	Auswertung	Client	Windows	Malware
Schadensausmaß	Auswertung	Client	Windows	Malware
Software-/Codevergleich	Auswertung	Client	Windows	Malware
Schädlingsidentifikation	Auswertung	Client	Windows	Malware
Verschlüsselungsablauf	Auswertung	Client	Windows	Malware
Cloud-Speicher	Auswertung	Client	Windows	Malware
Lokalisation	Auswertung	Client	Windows	Malware
Sicherheitslücken, Fernzugriffsmöglichkeiten	IT-Sicherheit	Client	Windows	Malware
Erstaufnahme, Beweisfragenformulierung	Vorbereitung	Client	Windows	Malware
Projektskizze	Vorbereitung	Client	Windows	Malware
IT-Infrastruktur	Vorbereitung	Client	Windows	Malware
zentraler Logserver	Vorbereitung	Client	Windows	Malware
Personennetzwerk	Vorbereitung	Client	Windows	Malware
Identifikation von Datenquellen, Triage	Vorbereitung	Client	Windows	Malware
Sicherung, Imaging	Vorbereitung	Client	Windows	Malware
Nämlichkeit	Vorbereitung	Client	Windows	Malware
Hardwarekomponenten	Vorbereitung	Client	Windows	Malware

Abbildung 18: Untersuchungsvorschlag für "Client, Windows, Malware"

Ein weiteres Beispiel:

Ein bestehender Untersuchungsplan für einen Fall von Datenabfluss auf einem Windows-Client (Anmerkung: der originale Untersuchungsplan liegt hier aus Vertraulichkeitsgründen nicht mehr vor, es handelt sich um eine während des Praxisprojekts erstellte Nachbildung eines originalen Untersuchungsplans):

1. Erstaufnahme
2. IT-Infrastruktur
3. Personennetzwerk
4. Datensicherung
5. Hashwertvergleich
6. Eventlogs
7. Registry
8. Systemzeit
9. Partitionierung
10. Betriebssystem
11. Dateiwiederherstellung/Carving
12. Suchindex
13. Stichwortsuche
14. Zeitstempelanalyse
15. Empfehlungen
16. Userdaten
17. E-Mails

Die Datenbankabfrage für diese Untersuchung sieht wie folgt aus:

```
use methodenbausteine;

select bausteine.BauName, bausteine.Bname, bauteine.BauVor-
aussetzung, objekte.ObjName, betriebssysteme.BSName, unter-
suchungsziel.ZielName

from bausteine, objekte, betriebssysteme, untersuchungs-
ziel, bau_obj, bau_bs, bau_ziel, bs_obj

 where    bausteine.BauIndex = bau_obj.BauIndex
 And bausteine.BauIndex = bau_bs.BauIndex
 And bausteine.BauIndex = bau_ziel.BauIndex
 And bau_obj.BauIndex = bau_bs.BauIndex
 And bau_obj.BauIndex = bau_ziel.BauIndex
 And bau_bs.BauIndex = bau_ziel.BauIndex
 And objekte.ObjIndex = bs_obj.ObjIndex
 And objekte.ObjIndex = bau_obj.ObjIndex
 And bs_obj.ObjIndex = bau_obj.ObjIndex
 And betriebssysteme.BSIndex = bau_bs.BSIndex
 And betriebssysteme.BSIndex = bs_obj.BSIndex
 And bau_bs.BSIndex = bs_obj.BSIndex
 And untersuchungsziel.ZielIndex = bau_ziel.ZielIndex
 And
        objekte.ObjName = "Client"
        And
        betriebssysteme.BSName = "Windows"
        And
        untersuchungsziel.ZielName = "Datenabfluss";
```

und liefert folgendes Ergebnis:

BauName	Bname	BauVoraussetzung	ObjName	BSName	ZielName
Hashwertvergleich	Allgemeines	zu vergleichende Daten vorhanden	Client	Windows	Datenabfluss
Hintergrundrecherchen	Allgemeines	Mehr Wissen benötigt	Client	Windows	Datenabfluss
Experimente	Allgemeines	Notwendigkeit für das Verstehen von Abläufen	Client	Windows	Datenabfluss
Softwareentwicklung	Allgemeines	Keine bereits existierende Software für das Pro...	Client	Windows	Datenabfluss
Datenanforderung	Allgemeines	Andere Datenquellen als Untersuchungserganz...	Client	Windows	Datenabfluss
Dateisystem	Aufbereitung	Sicherung	Client	Windows	Datenabfluss
Partitionierung	Aufbereitung	Sicherung	Client	Windows	Datenabfluss
Betriebssystem	Aufbereitung	Sicherung	Client	Windows	Datenabfluss
Rekonstruktion, Carving	Aufbereitung	gelöschte Dateien vermutlich vorhanden, ein Ne...	Client	Windows	Datenabfluss
Systemabbilder	Aufbereitung	System muss oder soll, beispielsweise wegen Ze...	Client	Windows	Datenabfluss
Wiederherstellung aus Backups	Aufbereitung	System muss oder soll, beispielsweise wegen Ze...	Client	Windows	Datenabfluss
Entschlüsselung	Aufbereitung	Verschlüsselung vorhanden, Passwortdokumente	Client	Windows	Datenabfluss
Filterung, Datenreduktion	Aufbereitung	Untersuchungsfragen klar	Client	Windows	Datenabfluss
Formatkonvertierung	Aufbereitung	Probleme bezüglich der Lesbarkeit von anderen ...	Client	Windows	Datenabfluss
Suchindex	Auswertung	Großer Fall, e-Discovery-Fall, Klarheit, wonach ...	Client	Windows	Datenabfluss
Erstsichtung	Auswertung	Entschlüsselung, falls verschlüsselt	Client	Windows	Datenabfluss
Live-Forensik	Auswertung	Notwendigkeit von Incident Response oder „ers...	Client	Windows	Datenabfluss
laufende Prozesse	Auswertung	Live-forensische Untersuchung	Client	Windows	Datenabfluss
Arbeitsspeicher	Auswertung	Live-forensische Untersuchung	Client	Windows	Datenabfluss
Post-mortem-Analyse	Auswertung	Sicherung	Client	Windows	Datenabfluss
Malwareprüfung	Auswertung	Malwarebefall vermutet	Client	Windows	Datenabfluss
User	Auswertung	Ursachenforschung	Client	Windows	Datenabfluss
Software	Auswertung	Ursachenforschung	Client	Windows	Datenabfluss
externe Geräte	Auswertung	Datentransfer vermutet	Client	Windows	Datenabfluss
Sitzungsdaten	Auswertung	Ursachenforschung	Client	Windows	Datenabfluss
Kommunikationsprotokolldaten	Auswertung	Ursachenforschung	Client	Windows	Datenabfluss
Systemzeit	Auswertung	Ursachenforschung	Client	Windows	Datenabfluss
Systemaktivitäten, Eventlogs	Auswertung	Ursachenforschung	Client	Windows	Datenabfluss
Registry	Auswertung	Ursachenforschung	Client	Windows	Datenabfluss
Konfigurationsdateien	Auswertung	Ursachenforschung	Client	Windows	Datenabfluss
Stichwortsuche	Auswertung	Beweisfragen und Untersuchungsziele sind klar	Client	Windows	Datenabfluss
Dateisignaturprüfung	Auswertung	Manipulation vermutet	Client	Windows	Datenabfluss
Metadaten	Auswertung	interessante, prüfbare Dateien vorhanden	Client	Windows	Datenabfluss
Erweiterte Attribute	Auswertung	Verdacht auf versteckte Dateien	Client	Windows	Datenabfluss
Fileslack-Analyse	Auswertung	Prüfung auf Restexistenz relevanter Dateien no...	Client	Windows	Datenabfluss
Internetaktivität	Auswertung	Ursachenforschung	Client	Windows	Datenabfluss
E-Mail-Client, Webmailer	Auswertung	Interessanter Kontakt zwischen zwei oder mehr...	Client	Windows	Datenabfluss
Plausibilisierung, Zeitstempelanalyse	Auswertung	Ursachenforschung	Client	Windows	Datenabfluss
Audio-, Video- und Bilddateien	Auswertung	Bestimmte Dateien werden gesucht	Client	Windows	Datenabfluss
Täterprofilanalyse	Auswertung	Es gibt Hinweise auf einen Täter und Spuren, a...	Client	Windows	Datenabfluss
Schadensausmaß	Auswertung	Opfer erleidet Datenverlust	Client	Windows	Datenabfluss
Software-/Codevergleich	Auswertung	Verdacht auf Diebstahl geistigen Eigentums	Client	Windows	Datenabfluss
Cloud-Speicher	Auswertung	Der Anspruch ist eine vollständige Datenerhebung	Client	Windows	Datenabfluss
Lokalisation	Auswertung	Die IP-Adresse oder die GPS-Koordinaten sind n...	Client	Windows	Datenabfluss

Abbildung 19: Untersuchungsvorschlag: "Client, Windows, Datenabfluss" Teil 1

Sicherheitslücken, Fernzugriffsmöglichkeiten	IT-Sicherheit	Sicherheitsvorfall	Client	Windows	Datenabfluss
Erstaufnahme, Beweisfragenformulierung	Vorbereitung	Auftrag	Client	Windows	Datenabfluss
Projektskizze	Vorbereitung	großes Projekt, e-Discovery-Fall, Incident Resp...	Client	Windows	Datenabfluss
IT-Infrastruktur	Vorbereitung	großes Projekt, e-Discovery-Fall, Incident Resp...	Client	Windows	Datenabfluss
zentraler Logserver	Vorbereitung	großes Projekt, e-Discovery-Fall, Incident Resp...	Client	Windows	Datenabfluss
Personennetzwerk	Vorbereitung	großes Projekt, e-Discovery-Fall, Incident Resp...	Client	Windows	Datenabfluss
Identifikation von Datenquellen, Triage	Vorbereitung	Datenquellen sind nicht eindeutig, IT-Infrastruk...	Client	Windows	Datenabfluss
Sicherung, Imaging	Vorbereitung	Notwendige Soft- und Hardware für Sicherung ...	Client	Windows	Datenabfluss
Nämlichkeit	Vorbereitung	Erstaufnahme, Beweisfragenformulierung, Iden...	Client	Windows	Datenabfluss
Hardwarekomponenten	Vorbereitung	Identifikation von Datenquellen	Client	Windows	Datenabfluss

Abbildung 20: Untersuchungsvorschlag: "Client, Windows, Datenabfluss" Teil 2

Insgesamt werden auch hier alle Punkte aus dem ursprünglichen Untersuchungsplan mit ausgegeben:

Erstaufnahme als „Erstaufnahme, Beweisfragenformulierung“

1. IT-Infrastruktur als „IT-Infrastruktur“
2. Personennetzwerk als „Personennetzwerk“
3. Datensicherung als „Datensicherung“
4. Hashwertvergleich als „Hashwertvergleich“
5. Eventlogs als „Systemaktivitäten, Eventlogs“
6. Registry als „Registry“
7. Systemzeit als „Systemzeit“
8. Partitionierung als „Partitionierung“
9. Betriebssystem als „Betriebssystem“
10. Dateiwiederherstellung/Carving als „Rekonstruktion, Carving“
11. Suchindex als „Suchindex“
12. Stichwortsuche als „Stichwortsuche“
13. Zeitstempelanalyse als „Plausibilisierung, Zeitstempelanalyse“
14. Empfehlungen – nicht mehr vorhanden
15. Userdaten als „User“
16. E-Mails als „E-Mail-Client, Webmailer“

Es ist zu sehen, dass insgesamt mehr Bausteine als eigentlich nötig ausgegeben werden. Zwar sind insgesamt alle Bausteine vorhanden, die auch im ursprünglichen Untersuchungsplan vorhanden waren, allerdings waren die Untersuchungspläne vorher bereits bekannt und wurden verwendet, was das Ergebnis unter Umständen beeinflusst.

4 Diskussion, Fazit und Ausblick

4.1 Zusammenfassung und Interpretation

Die Beantwortung der anfangs gestellten Fragen und die Bestätigung der Hypothesen wurden durch vertiefende Literaturrecherchen, dem Interview mit Alexander Sigel, DigiTrace GmbH und der daraus resultierenden Neuerstellung von Bausteinen und der ergänzenden Modellierungen der Bausteine erreicht.

Die Bausteine weisen durch ihre Zuordnung zu einzelnen Spalten (Name, Beschreibung, Bereich, Voraussetzung, Ziel, Artefakt, Methode, Objekt, Betriebssystem und Untersuchungsziel) eine Standardisierung und auch Konsistenz auf. Die Inhalte der einzelnen Zuordnungen sind variabel und nicht statisch, weshalb auf zukünftige, beispielsweise technische, Veränderungen reagiert werden kann. Natürlich können die Bausteine angepasst werden, falls sie an der ein oder anderen Stelle noch nicht rund in das Bauplansystem passen sollten. Durch die zielgerichtete Abfrage nach bestimmten Problemen auf bestimmten Objekten mit bestimmten Betriebssystemen können Fehler vermieden, beziehungsweise minimiert werden. Die Bausteine sind jetzt ziemlich umfassend gestaltet, was es dem Untersuchenden ermöglicht, potentielle nächste oder vergessene Untersuchungsschritte im Überblick schnell zu erkennen und die Bausteinlisten als Gedankenstütze oder Checkliste zu nutzen. Zusätzlich wird für jeden Baustein eine geeignete Methode im Bezug auf die Auswertung beschrieben, sodass man hier erkennen kann, wie dieser Schritt durchgeführt werden sollte.

4.2 Erzielte Fortschritte

Insgesamt sind folgende Ziele ausgehend von dem Exposé erreicht worden: Erfahrungswissen aus der Praxis und der Literatur konnte extrahiert und mit in die Bausteinliste aufgenommen werden. Die Serienanfertigung von Untersuchungsplänen kann jetzt getestet werden.

Eine neue Kategorie „IT-Sicherheit“ konnte erstellt werden und erhielt ebenfalls zwei erste grobe Bausteine. Die Granularität der Bausteine konnte angepasst und die Bausteine konnten für bestimmte IT-forensische Fragestellungen bedingt zugeschnitten werden. Auf die Erweiterung der Spalte „Betriebssystem“ wurde verzichtet, da die

meisten Bausteine nicht betriebssystemabhängig sind, was aufgrund der Schnelligkeit, in der sich Technik verändert, nicht gewünscht war.

Es konnten gänzlich neue Bausteine generiert werden, die in ihrer Existenz die IT-forensischen Untersuchungspläne erweitern, ergänzen und ihre Genauigkeit erhöhen. Untersuchungsziele und -fragen konnten aus Literatur, bereits vorhandenen DigiTrace-Untersuchungsplänen und einem Interview herausgefiltert werden. Die wichtigsten wurden sowohl zusammengefasst als auch in der Spalte „Untersuchungsziel“ ergänzend hinzugefügt. Jeder Baustein verfügt über verschiedene Untersuchungsziele für die er eingesetzt werden kann. Durch die zusätzlichen Bausteine und durch die Erweiterung der Kategorien „Objekt“ und „Untersuchungsziel“ hat sich die Datenbank verändert und somit auch ihre Abfragen und Abfragemöglichkeiten.

Die Bausteine erhielten durch die neu hinzugefügte Spalte „Voraussetzung“ Beziehungen zu einander, welche einen schnellen Überblick darüber verschaffen, ob ein bestimmter geplanter Untersuchungsschritt noch einen anderen, vorangestellten Untersuchungsschritt benötigt oder unter welchen Voraussetzungen dessen Durchführung sinnvoll ist. Auch sind in dieser Spalte generelle Situationen aufgelistet, die den Verwendungszweck des Bausteins auf ein wesentliches vorher existierendes Problem herunterbrechen. Bestimmte Bausteine konnten bestimmten Problemen zugeordnet werden und stellen somit einen Ansatz für die Erstellung von Regeln dar.

Im Gegensatz zum Praxisprojekt, welches zunächst eine Art Machbarkeitsstudie für die Erstellung von einzelnen Untersuchungsbausteinen im Allgemeinen darstellte, können jetzt mehr Fälle abgedeckt werden, da die Bausteinliste sowohl mehr Fälle und Objekte als auch mehr Bausteine an sich umfasst. Allerdings muss dazu gesagt werden, dass die Bausteine nicht an aktuell neuen Fällen getestet wurden, weshalb die tatsächliche aktuelle Nutzbarkeit nicht oder nur auf Basis bereits vorher erstellter Untersuchungspläne festgestellt werden konnte.

4.3 Probleme und potentielle Lösungsansätze

Da die meisten der Bausteine über flächendeckende und unterschiedliche Informationen verfügen und somit in den verschiedensten Fällen eingesetzt werden können und/oder sollten, bleibt hier die erwünschte Diversität zur Unterscheidung verschiedener Fälle aus. Für viele Bausteine ist eine eineindeutige Zuordnung zu einem spezifischen Problem zum jetzigen Zeitpunkt nicht möglich, weshalb derjenige, dem der ausgegebene Untersuchungsvorschlag nützen soll, immer noch manuell Bausteine aus-

sortieren muss. Diese können zwar generell für das zu untersuchende Problem nützlich sein, sind aber aufgrund möglicher, vorangegangener, klar definierter Untersuchungsfragen nicht unmittelbar notwendig. Unterschiede in den ausgegebenen Untersuchungsplänen können bei der Betrachtung verschiedener Probleme festgestellt werden, allerdings sind die ausgegebenen Untersuchungspläne in ihrer Variabilität begrenzt.

Des Weiteren wurden viele Objekte bei Bausteinen beibehalten, die nicht primär für bestimmte Untersuchungsschritte und -ziele prädestiniert sind, allerdings können IT-technische Systeme mit dem nötigen Fachwissen modifiziert und zweckentfremdet werden, wie bereits erwähnt. Manuell aussortieren ist hier immer noch nötig. Der Abgleich zwischen den einzelnen Punkten erfolgte übergeneralisiert, was bedeutet, dass der Konfigurierende feststellen muss, ob der Baustein initial relevant ist. Wenn ein Untersuchungsschritt aber aufgrund von vorherigen Restriktionen gar nicht erst für ein bestimmtes Problem auftaucht, gerät er unter Umständen in Vergessenheit. In der vorgestellten Abfrage für die Malwareuntersuchung auf einem Windowsclient tauchen Untersuchungsschritte wie „Täterprofilanalyse“ auf, obwohl hier von Beginn an klar war, dass es sich um eine Untersuchung auf Malware handelt, die vermutlich ungerichtet stattfand. Dennoch kann man im Laufe der Untersuchungen auf Informationen stoßen, die einen später dazu veranlassen könnten eine solche Analyse oder eine „Lokalisation“ des Täters zu veranlassen.

Insgesamt sind die Untersuchungsbausteine und die daraus generierbaren Untersuchungspläne praktisch und sinnvoll, da sie zusammen eine umfassende Liste von Untersuchungsschritten für eine bestimmte angeforderte IT-forensische Analyse darstellen. Diese Liste ermöglicht eine Wissensweitergabe an Mitarbeiter und bietet zuverlässig Vorschläge für Untersuchungsschritte an. Aus den vorgeschlagenen Untersuchungsschritten müssen unter Umständen immer noch manuell einzelne Untersuchungsschritte selektiert werden, um die Individualität eines bestimmten Untersuchungsvorhabens besser fassen zu können. Durch die übergeneralisierte Beschreibung der Bausteine zu Beginn der Testphasen kann man sicher stellen, dass nichts vergessen geht und die Untersuchung ganzheitlich stattfinden kann. Die Erstellung von Untersuchungsplänen kann hierdurch deutlich effizienter gestaltet werden und somit Zeit und Geld sparen.

4.4 Vorschläge für weitere Arbeiten

Erstellung eigener Software war zwar nicht wesentlicher Bestandteil dieser Arbeit, allerdings wäre eine GUI für die Datenbank in Zukunft wünschenswert, um die Benutzerfreundlichkeit zu erhöhen. Momentan kann man zwar sehen, wo in der Abfrage das Betriebssystem, das Objekt und das Ziel definiert werden und es an diesen Stellen entsprechend anpassen, allerdings ist Code, in dem man ohne geeignete Benutzeroberfläche manuell Änderungen vornehmen muss, um seine Abfragen anpassen zu können, nicht benutzerfreundlich.

Des Weiteren wäre eine unterstützende Anwendung deshalb sinnvoll, notwendig und wünschenswert, weil sie die Pflege der Datenbank, die aktuell immer noch manuell durchgeführt wird, wesentlich erleichtern würde.

Nützlich hierfür könnte das Wissen aus dem Dokument „Case Domain Modeling“ sein, da diese wissenschaftliche Publikation sich insbesondere mit der Implementierung von Datenbanken mittels „Case Domain Modeling“ beschäftigt.

Ebenfalls sinnvoll wäre es die Bausteine fortwährenden Praxistests während der Erstellung von Untersuchungsplänen zu unterziehen, um sie aktuell zu halten, ihre Effektivität zu erhöhen, ihren Nutzen zu maximieren und festzustellen, ob manche Objekte oder Ziele für bestimmte Bausteine im Gegensatz zu vorherigen Annahmen doch gänzlich ungeeignet sind.

Man könnte die Bausteine nach erfolgreichen Testphasen in eines der unter 3. genannten oder in ein anderes Case-Management-Tool einbetten.

Um zu testen inwiefern sich die Ausgabe der Untersuchungspläne für eine Wissensweitergabe an unerfahrenere Forensiker eignet, könnte man diese mit entsprechenden Personen testen und im Nachgang von einer erfahrenen Person in diesem Bereich überprüfen lassen und daraus ein Gütemaß entwickeln. Für diese Tests und für eine Einbettung der Bausteine in ein Case-Management-System, wäre es sinnvoll den Aufwand für bestimmte Untersuchungsschritte, beispielsweise in Abhängigkeit zu einer zu untersuchenden Datenmenge, zu erheben. Getestet werden sollte ebenfalls welche Bausteine an welcher Stelle initial relevant sind, um die vorgeschlagenen Untersuchungsschritte noch genauer anpassen zu können. Im Zuge dieser Tests sollte die Wartung und Fortschreibung wieder neue Fragen auf Erweiterungen und Anpassungen nach sich ziehen.

Literaturverzeichnis

1: SIGEL, Alexander (2017): Exposé für die Bachelorarbeit: Wiederverwendbare Methodenbausteine zur Konfiguration IT-forensischer Untersuchungspläne, erstellt am 23.08.2017

2: DETTMAR, Meike (2017): Praxisprojekt-Bericht - Wiederverwendbare Methodenbausteine zur Konfiguration IT-forensischer Untersuchungspläne, eingereicht am 12.05.2017, Hochschule Mittweida - University of Applied Sciences

3: Bundesamt für Sicherheit in der Informationstechnik (2011): Leitfaden IT-Forensik, Version 1.0.1 (März 2011), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2, zuletzt aufgerufen am 24.11.2017

4: MAIR, Karin; MARKO, Roland & REITER, Lukas (2013): Forensische Nutzung von IT und Daten, Vortragsfolien vom 24.05.2013, https://www.infolaw.at/downloads/mag_karin_mair_cfe_et_al-forensische_nutzung_von_it_und_daten-2013-05-23.pdf, zuletzt aufgerufen am 24.11.2017

5: HAILEY, Steve (2002): What Is Computer Forensics?, veröffentlicht am 02.04.2002, in: *Cybersecurity Institute*, http://www.cybersecurityinstitute.biz/forensics.htm, zuletzt aufgerufen am 24.11.2017

6: PURUSHOTHAMAN, Dr. K. & HASHEMNEJAD, Dr. R. (2013): Cyber Forensic Investigation Plan, in: *International Journal of Advance Research*, IJOAR.org, ISSN: 2320-9194, https://www.academia.edu/3827683/Cyber_Forensic_Investigation_Plan, zuletzt aufgerufen am 24.11.2017

7: SANSUROOAH, Krishnun (2006): Taxonomy Of Computer Forensics Methodologies And Procedures for Digital Evidence Seizure, in: *Australian Digital Forensics Conference – Conferences, Symposia and Campus Events*, Edith Cowan University – Research Online, http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1031&context=adf, zuletzt aufgerufen am 24.11.2017

8: NIMSGER, Kristin M. & LANGE, C.S. Michele (2002): Examining the Data, A beginners guide to computer-based evidence, https://www.krollontrack.com/publications/securityproducts.pdf, zuletzt aufgerufen am 24.11.2017

9: SITI RAHAYU, Selamat; ROBIAH, Yusof & SHAHRIN, Sahib (2008): Mapping Process of Digital Forensic Investigation Framework, Faculty of Information Technology and Communication, Universiti Teknikal Malaysia Melaka, Ayer Keroh, Melaka, Malaysia, 2008, in: *IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, October 2008* http://paper.ijcsns.org/07_book/200810/20081025.pdf, zuletzt aufgerufen am 24.11.2017

10: CICHONSKI, Paul; MILLAR Tom; GRANCE, Tim & SCARFONE, Karen: Computer Security Incident Handling Guide (Draft) - Recommendations of the National Institute of Standards and Technology (2012), Special Publication 800-61 Revision 2, in: *NIST (National Institute of Standards and Technology – U.S. Departmend of Commerce)*,

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf, zuletzt aufgerufen am 24.11.2017

11: RIST, Oliver (2002): Developing a Response Plan for Computer Forensics, veröffentlicht am 22.02.2002 in *Enterprise Networking Planet*, http://www.enterprisenetworkingplanet.com/netsecur/article.php/979231/Developing-a-Response-Plan-for-Computer-Forensics.htm, zuletzt aufgerufen am 24.11.2017

12: Atoz Gossips (2016): Digital Forensics Investigation Plan, Bericht in *Atoz Gossips*, veröffentlicht am 27.05.2016, http://atozgossips.com/2016/05/27/digital-forensics-investigation-plan/, zuletzt aufgerufen am 24.11.2017

13: Course Technology – CENGAGE Learning (2010): Computer Forensics - Evidence Collection & Preservation, EC-Council | Press, Volume 1 of 5 mapping to CHFI (Computer Hacking Forensic INVESTIGATOR) Certification, https://zodml.org/sites/default/files/Computer_Forensics.pdf, zuletzt aufgerufen am 24.11.2017

14: PHELPS, James (2013): Digital Evidence Collection Training for Law Enforcement - Computer Forensics and Digital Evidence, 2013, Vortragsfolien, Angelo State Universtiy http://www.depts.ttu.edu/cs/research/csecs/workshop/docs/2014/Forensics/SCSW-Forensics-Phelps.pdf, zuletzt aufgerufen am 24.11.2017

15: LEONG, Ricci Sze-Chung (2006): FORZA: Digital Forensics Investigation Framework That Incorporate Legal Issues, in *DFRWS: Digital Forensic Research Conference – DFRWS 2006 USA – Lafayette (Aug 14th – 16th),* https://dfrws.org/sites/default/files/session-files/paper-forza_-_digital_forensics_investigation_framework_that_incorporate_legal_issues.pdf, zuletzt aufgerufen am 24.11.2017

16: LOTHRIDGE, Kevin & FITZPATRICK, Frank (2013): Crime Scene Investigation: A Guide for Law Enforcement (BJA, NIJ – National Institute of Justice, NIST, nfstc), original guide developed and approved by the Technical Working Group on Crime Scene Investigation, January 2000, Updated guide developed and approved by the Review Committee, September 2012, National Forensic Science Technology Center, https://www.nist.gov/sites/default/files/documents/forensics/Crime-Scene-Investigation.pdf, zuletzt aufgerufen am 24.11.2017

17: POLLITT, Mark (2006): Applying Traditional Forensic Taxonomy To Digital Forensics, Chapter 2 – Auszug aus einem wissenschaftlichen Paper, https://pdfs.semanticscholar.org/5b56/e55545ef362625164d4ed4c3debd74ebe817.pdf, zuletzt aufgerufen am 24.11.2017

18: HANNAN, Mathew & TURNER, Dr. Paul (2003): Australian Forensic Computing Investigation Teams: Research on Competence, School of Information Systems, University of Tasmania, Australia, https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwjHrqLFttDXAhVJIOwKHRznAQMQFgg4MAI&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.474.7257%26rep%3Drep1%26type%3Dpdf&usg=AOvVaw0k7EXjQdEY0mhmyR2UsvRP, zuletzt heruntergeladen am 24.11.2017

19: PONN, Josef; BRAUN, Thomas & LINDEMANN, Udo (2004): Zielgerichtete Produktentwicklung durch modulare Prozessstrukturen und situationsgerichtete Methodenauswahl, in: *15. Symposium „Design For X", Neukirchen, 14. und 15. Oktober 2004*, https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwjhi8TwnNb

XAhUhL8AKHVS0B1AQFgg0MAE&url=https%3A%2F%2Fwww.designsociety.org%2Fdownload-publication%2F27620%2Fzielgerichtete_produktentwicklung_durch_modulare_prozessstrukturen_und_situationsgerechte_methodenauswahl&usg=AOvVaw1UfgOJ9QqYuz9phR30bG8g, zuletzt heruntergeladen am 24.11.2017

20: BOGEN, Alfred C.; DAMPIER, David A.; CARVER, Jeffrey C. (2007): Support for Computer Forensics Examination Planning with Domain Modeling: A Report of One Experiment Trial, in: *Proceedings of the 40th Hawaii International Conference on System Sciences - 2007*, https://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwiB-ubWndbXAhUiDsAKHYXMB04QFggwMAE&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.96.1581%26rep%3Drep1%26type%3Dpdf&usg=AOvVaw25A-BfbnDcAqpc9Ke78iVu, zuletzt heruntergeladen am 24.11.2017

21: SCHNEIER, Bruce (1999): Attack Trees, in: *Dr. Dobb's Journal*, December 1999, https://www.schneier.com/academic/archives/1999/12/attack_trees.html, zuletzt aufgerufen am 24.11.2017

22: BRUSCHI, Danilo; MONGA, Mattia & MARTIGNONI Lorenzo (2005): How to Reuse Knowledge about Forensic Investigations, *in: DFRWS (Digital Forensic Research Conference), DFRWS 2004 USA – Baltimore, MD (Aug 11th – 13th)*, https://www.dfrws.org/conferences/dfrws-usa-2004/sessions/how-reuse-knowledge-about-forensic-investigations, Attachement 1 (Size: 314,14KB), zuletzt heruntergeladen am 24.11.2017

23: GREGG, Brandon (2010): Whodunnit? 5 free or cheap tools to manage investigations, veröffentlicht am 18.08.2010, *Onlineartikel von CSO (from IDG)*, https://www.csoonline.com/article/2125881/investigations-forensics/whodunnit-5-free-or-cheap-tools-to-manage-investigations.html, zuletzt aufgerufen am 24.11.2017

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe. Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Ort, den TT. Monat JJJJ Vorname Nachname